Exhibit A

Payment Card Industry (PCI)
Data Security Standard

Final PFI Report

INNOAS, Inc.
September 2017
v1.0

Foregenix Inc.
60 State Street, Boston,
Massachusetts, USA
+15086441504

Confidentiality Notice

Applied Conventions

Please note the following conventions that are used throughout Foregenix' reports.

- All timestamps are converted to and presented in UTC unless otherwise specified.
- Timestamps will be presented in a zero padded 24-hour clock format.
- Dates will be presented in full, i.e. August 17th 2016 or ISO8601 (YYYY-MM-DD) format e.g. 2016-08-17.
- Timestamps with date information will be presented in ISO8601 format i.e. 2016-08-17T14:22:39.

Table of Changes

Company Name	Name / Title	Date	Version	Description

Table of Contents

Index of Tables

Index of Illustrations

1 Contact Information and Executive Summary

Summary of Investigation

On March 22nd, 2017, Foregenix was first contacted by INNOAS, Inc. a Point of Sale service provider, with a request for information on investigative services. On May 31st, 2017, Foregenix Inc. was re-engaged by Jake Lee, a member of Operations for INNOAS, Inc. to respond to an incident regarding a compromise of several merchant Point of Sale (POS) environments which they manage. Contracts were provided on April 21st, 2017 and then were fully executed on May 31st, 2017, and the investigation commenced on May 31st, 2017. The proceeding sections of this report provide a high-level summary of the investigation and analysis performed by Foregenix Inc.

An intrusion was confirmed prior to the investigation and it was determined that it originated from compromised remote access facility *LogMeIn* which is used for remote support of the service provider's merchant environment(s). Once the unauthorized access was gained to the service provider's *LogMeIn* portal, intruders proceeded to install malware on several Point of Sale terminals within the various merchant's Point of Sale (POS) environments. While conclusive evidence of a data compromise was discovered by INNOAS, Inc., Foregenix was also tasked with the following objectives:

- Forensic Analysis
- Malware-Virus Analysis
- File System Analysis
- Data Extraction
- Database Analysis
- Sensitive Data Exfiltration
- Log Analysis

Overview of Findings

At the request of Mastercard, a PFI investigation was to be conducted on a sampling of merchant locations. Based on the client list provided by INNOAS, Inc., Foregenix along with the Mastercard, *Elavon*, and *FristData* selected a sample set of locations for full PFI examination based on those which had been flagged by positive Common Point of Purchase (CPP) reports. These locations are listed below in Table 1, highlighted in red. With reference to coverage of the remaining locations, Foregenix deployed our Incident Response technology *Serengeti* for rapid initial assessment and ongoing monitoring. Foregenix shipped evidence acquisition drives and forensic imaging tools to the respective locations for gathering evidence under the direction of Foregenix.

On May 25th, 2017, an incident responder from Foregenix worked with Jake Lee at the *Caffe Bene* Boston located on 333 Massachusetts Avenue, Boston Massachusetts to review the process for collecting forensic evidence. While on-site, Foregenix observed that this particular merchant's customer wireless Internet access (WiFi) was on the same network as the Point of Sale devices. Foregenix strongly recommended to the merchant as well as INNOAS, Inc. that these networks need to be separated and is in violation of PCI-DSS while also puts the merchant at a greater risk to being breached from within.

Jake Lee obtained a recorded video *LogMeIn* session from one of the merchant's locations (*Global Kitchen*), and this video clearly showed an unauthorized user downloading malware from a remote host [`http://146.0.77.8/1.zip`] located in the Netherlands on December 17th, 2016. While the unauthorized user was extracting the files, *Microsoft Security Essentials* did detect and quarantined the malware. The unauthorized user proceeded to adjust the anti-virus settings of the device to allow the full extraction and execution of the malicious content. The source of the logon was from the IP address `64.120.44.139` a host located in Phoenix Arizona registered with *Nobis Technology Group, LLC* a web hosting company. The original intrusion for this(*Global Kitchen*) location occurred on December 16th, 2017. According to Jake Lee, multi-factor authentication was enabled for remote access. INNOAS, Inc. claimed that the unauthorised "individual" would intercept the multi-factor email message and

would processed and succeed with the login. Unfortunately, log data that could have provided evidence to validate this assertion was not available.

Further analysis on the *LogMeIn* remote access logs indicated that the first instance this intruder gained access to the profile was on December 9th, 2016. Based on these logs, unauthorized access was established up until December 17th, 2016; however, during this time period it is unclear precisely what the unauthorized user was doing on the host systems as audit records do not provide this level of context regarding user activity. Furthermore, all systems that had been accessed by the intruder were redeployed by INNOAS, Inc. destroying evidence and negating the possibility of forensic analysis.

Based on a forensic review of the sites listed in red, it was determined that a considerable amount of clean-up had occurred prior to engaging a forensic firm. File traces of the malware and IP address in question were detected through forensic processing, and Foregenix suspects that all sites infected underwent this same clean-up effort, possibly to contain the situation. it should be noted that no storage of card holder data was reflected on any of the systems reviewed. Locations listed within Table 1as "unknown" (Containment and Intrusion Start Dates) had no data to support a system compromise, therefore it is unknown to Foregenix if these sites were in fact accessed in an unauthorized manner or inpacted. Exact containment dates could not be distinguished by INNOAS, Inc. as service records were not kept. Best estimate insight provided by Jake Lee related to mid January 2017, as indicated in the table below, additionally, the remote access facility was changed to *TeamViewer* professional with multi-factor authentication enabled in January 2017.

Legal Name	DBA Name	Address	City	State	Processor Acquirer	Intrusion Start Date	Containment Date
CB 17th Street LLC	Caffe Bene MPD	300 W. 17th St.	New York	NY	Elavon	2016-12-10	January 2017
House of Caffe Bene, Inc.	Caffe Bene 157th	9 Edward Morgan Pl.	New York	NY	Elavon	2016-12-14	January 2017
GKNY1 Inc.	Global Kitchen	52 W. 52nd St.	New York	NY	First Data	2016-12-16	January 2017
R & G Soho, LLC	Piccola Cucina Spring	196 Spring St.	New York	NY	Chase Paymentech	2016-12-10	January 2017
KEO BOO KEE Corp.	BBQ Cliffside Park	651 Anderson Ave	Cliffside Park	NJ	First Data	2016-12-13	January 2017
Chen & Chen Brothers Inc.	Caffe Bene Boston	333 Massachusetts Ave.	Boston	MA	Elavon	2016-12-10	January 2017
Pinnacle Bar & Grill	Cast Iron Pot	356 Bergen Blvd.	Fairview	NJ	Bankcard Service Merrick Bank	2016-12-17	January 2017
June & Shana, Inc.	Caffe Bene Sunnyside	41-31 Queens Blvd.	Sunnyside	NY	Elavon Merrick Bank	2016-12-14	January 2017
Lucky Star Caffe Inc.	Caffe Bene Brooklyn 18th	6307 18th Ave.	Brooklyn	NY	Elavon	2016-12-10	January 2017
Lee & Lim, LLC	BBQ Flushing	158-23 Northern Blvd.	Flushing	NY	Elavon	2016-12-09	January 2017
BBQ Chicken Little Neck Corp.	BBQ Little Neck	251-16 Northern Blvd.	Little Neck	NY	First Data	Unknown	Unknown
725 Thrid Avenue Corp.	Bocca Bliss	725 3rd Ave	New York	NY	Elavon	2016-12-17	January 2017
Jamo 26, Inc.	Izakaya Nomad	13 W.26th St.	New York	NY	First Data	2016-12-10	January 2017
R & G Soho, LLC	Piccola Cucina Prince	184 Prince St.	New York	NY	Chase Paymentech	2016-12-17	January 2017

Legal Name	DBA Name	Address	City	State	Processor Acquirer	Intrusion Start Date	Containment Date
Gogi, Inc.	Soju Haus	315 5th Ave. 2Fl	New York	NY	Elavon	2016-12-10	January 2017
Amber Nail & Spa, Inc.	Amber Nail Bronx	3011 Middletown Rd.	Bronx	NY	Elavon	Unknown	Unknown
Blooming Nail and Foot Spa Inc.	Blooming Nail	614 624 Mamaroneck Ave	White Plains	NY	Elavon Merrick Bank	Unknown	Unknown
Gel Factory Corp.	Gel Factory	3051 Jericho TPKE.	East Northport	NY	First Data	Unknown	Unknown
Peggie Nail Inc.	Peggie Nail	416 3rd Ave.	New York	NY	Elavon	Unknown	Unknown
Town Nail & Foot Spa Inc.	Town Nail	450 Central Park Ave.	Scarsdale	NY	POS Maintenance Only	Unknown	Unknown
Samhyungjae Corp.	Starry Night	28 West 33rd Street	New York	NY	Elavon	Unknown	Unknown
Damoa Union Inc.	Damoa	36-44 Union St. FL 1	Flushing	NY	Elavon	Unknown	Unknown
Pak Cafe Bene, LLC	Caffe Bene Jersey City	77 Hudson St.	Jersey City	NJ	Elavon	2016-12-15	January 2017
Caffe Bene Fort Lee LLC	Caffe Bene Fort Lee	1636 Palisade Ave #5,6	Fort Lee	NJ	First Data	2016-12-14	January 2017
Soonmyung Development Corp.	Caffe Bene New Brunswick	356 George ST.	New Brunswick	NJ	Elavon	2016-12-14	January 2017
Kenny Baek Corp.	BBQ Old Tappan	216 Old Tappan Rd. #A6	Old Tappan	NJ	First Data	2016-12-15	January 2017
Wally's Hot Bagels, LLC	Wally's	258 Closterdock Rd.	Closter	NJ	First Data	2016-12-17	January 2017
Taste Treat LLC	Boomboom Rutherford	36A Park Ave	Rutherford	NJ	First Data	Unknown	Unknown
BC of God	Boomboom Edison	1751 Lincoln Hway	Edison	NJ	First Data	2016-12-17	January 2017
Namgung Corp.	Crome Fort Lee	1640 Schlosser St.	Fort Lee	NJ	POS Maintenance Only	2016-12-10	January 2017
Spoon & Chopstick LLC	Omori Food System	520 Bergen Blvd. STE 9	Palisades Park	NJ	Elavon	Unknown	Unknown
Spa Reee Inc.	Angel Tips Gillette	977 Valley Rd	Gillette	NJ	Elavon	Unknown	Unknown
J & J Bloom Spa, Inc.	Bloom Spa Springfield	901 Mountain Ave.	Springfield	NJ	First Data Merrick Bank	Unknown	Unknown
Casino Car Wash, Inc.	Casino Car Wash	425 Grand Ave	Palisades Park	NJ	Elavon	2016-12-09	January 2017
PHK Co, Inc.	Rokman	241 Commercial Ave.	Palisades Park	NJ	First Data Elavon	2016-12-09	January 2017
Classique I Dayspa, Inc.	Classique Day Spa	32 E. Prospect Ave	Waldwick	NJ	POS Maintenance Only	2016-12-15	January 2017

Legal Name	DBA Name	Address	City	State	Processor Acquirer	Intrusion Start Date	Containment Date
J Beauty Spa Corp.	J Nail	265 Grove St.	Jersey City	NJ	Elavon	Unknown	Unknown
Dream Nail & Spa, Inc.	Grace Nail & Spa	48 Essex St.	Jersey City	NJ	First Data	Unknown	Unknown
Ohnas Corp.	Paradise Nail	197 Route 202-206 South	Bedminster	NJ	POS Maintenance Only	Unknown	Unknown
Bloom Spa, Inc.	Bloom Spa Hoboken	402 Washington St.	Hoboken	NJ	First Data	Unknown	Unknown
Lemoine Gateaux Bakery LLC	Café Gateaux Fort Lee	2175 Lemoine Ave. Suite 101	Fort Lee	NJ	Elavon	Unknown	Unknown
Gateaux Bakery Corp.	Café Gateaux Closter	570 Piermont Rd.	Closter	NJ	First Data	Unknown	Unknown
TLJ Ridgefield Inc.	Café Gateaux Ridgefield	321 Broad Ave.	Ridgefield	NJ	First Data	Unknown	Unknown
Café Nomis Inc.	Café Nomis	493 Broadway	Bayonne	NJ	Elavon	Unknown	Unknown
Abies Corporation	Caffe Bene Ellicott City	10039 Baltimore National Pike #E	Ellicott City	MD	Elavon	2016-12-10	January 2017
Caffe Bene Champaign Inc.	Caffe Bene Urbana	700 S. Gregory St. STE1	Urbana	IL	Elavon	2016-12-13	January 2017
Caffe Bene Midwest LLC.	Caffe Bene Glenview	1741 N. Milwaukee Ave.	Glenview	IL	Elavon	2016-12-13	January 2017
Caffe Bene Green Inc.	Caffe Bene Champaign	524 E. Green St.	Champaign	IL	Elavon	2016-12-10	January 2017
KimcrystalMin Inc.	Caffe Bene Suwanee	295 Edgewater Dr.	Macon	GA	Elavon	2016-12-10	January 2017
R & G Espanola, LLC	Piccola Cucina Miami	440 Espanola Way	Miami Beach	FL	POS Maintenance Only	2016-12-10	January 2017
Bae & Kim, Inc.	Caffe Bene Buena Park	5401 Beach Blvd.	Buena Park	CA	Elavon	2016-12-13	January 2017
Nabee Inc.	Caffe Bene Western	607 S. Western Ave.	Los Angeles	CA	First Data	2016-12-10	January 2017
Kafferia, Inc.	Caffe Bene Wilshire	3287 Wilshire Blvd #B	Los Angeles	CA	Elavon	2016-12-14	January 2017
JihoJiwoo, Inc.	Caffe Bene Rowland HTS	18716 Colima Rd.	Rowland Heights	CA	Elavon	2016-12-10	January 2017
MCKN Enterprise, Inc.	Caffe Bene San Diego	4620 Convoy St.	Sandiego	CA	Elavon	2016-12-09	January 2017
San Marino Caffebene Inc.	Caffe Bene San Marino	2322 Huntington Dr.	San Marino	CA	Elavon	2016-12-09	January 2017
Carrot House Inc.	Caffe Bene Carrollton	1016 W Trinity Mills Rd Ste 100	Carrollton	TX	First Data	2016-12-10	January 2017
Moonstone Nail & Spa	Moonstone Spa	2650 King Rd. STE 800	Frisco	TX	Elavon	Unknown	Unknown
Anlaur, Inc.	Cuticle Corner Berwyn	408 W. Swedesford Rd.	Berwyn	PA	POS Maintenance Only	Unknown	Unknown

Legal Name	DBA Name	Address	City	State	Processor Acquirer	Intrusion Start Date	Containment Date
29 Iris Nail and Spa, Inc.	Iris Nail Lansdale	29 E. Hancock St.	Lansdale	PA	First Data	Unknown	Unknown
Caffe Bene Ktwon Inc.	Caffe Bene 32th	39 W. 32nd St.	New York	NY	Elavon	2016-12-15	January 2017
Cibam Inc.	Caffe Bene Astoria	3214 Steinway St.	Astoria	NY	Elavon	2016-12-15	January 2017

Table 1: Expanded Site Status

This assessment does not comprise a formal PCI security audit and may not be fully representative of the INNOAS, Inc. security posture or the security posture of the merchants to which they provide service. A Qualified Security Assessor (QSA) should be appointed to perform a formal PCI gap analysis with detailed recommendations after which corrective actions can be addressed.

1.1 Contact Information

Client Information			
Company Name	INNOAS, Inc.	SSC Case Reference Number	360100
Company Address	21 Grand Avenue Suite 111 Palisades Park, NJ 07650		
Company URL	http://www.innoas.com		
Company Contact Name	Jake Lee		
Contact Phone Number	(201) 905-3521		
Contact eMail Address	jake.lee@innoas.com		
Acquiring Bank Information			
Acquirer Name	Not applicable		
Acquirer Address	Not applicable		
Acquirer Contact	Not applicable		
Acquirer Contact Phone Number	Not applicable		
Acquirer Contact eMail Address	Not applicable		
Has the Acquirer(s) been notified	Not applicable		
PFI Company			

PFI Company Name	Foregenix Inc.
PFI Company Address	60 State Street, Boston, Massachusetts, USA
PFI Company URL	http://www.foregenix.com
PFI Employee	
PFI Employee Name	Sterling Thomas
PFI Employee Phone Number	615-295-0295
PFI Employee eMail Address	sthomas@foregenix.com
PFI Case Reference Number	FGX-201705-360U
Card Brand Case Reference Numbers	
American Express Reference	C1704011217
Discover / Diners Reference	Unknown at this time
JCB Reference	Unknown at this time
MasterCard Reference	ADC-002772-17
VISA Reference	Unknown at this time

1.2 Brand Acceptance

Card Brand Acceptance	
VISA	☐ YES ☒ NO
MasterCard	☐ YES ☒ NO
Discover / Diners	☐ YES ☒ NO
American Express	☐ YES ☒ NO
JCB	☐ YES ☒ NO
Other	☒ YES ☐ NO
If other, identify other brand acceptance	INNOAS, Inc.. is a Point of Sale (POS) integrator that does not accept cards directly. They administer POS systems on behalf of merchants that do accept card transactions.

1.3 Date and Timeframe of Assessment

Engagement Timing	
Date of PFI Company Engagement	May 31st, 2017, contracts were officially signed. INNOAS, Inc. original contacted Foregenix on March 20th, 2017, to discuss what the PFI process entailed.
Date Forensic Investigation Began	May 31st, 2017

1.4 Locations Reviewed

Location(s)	On site Investigation	Remote Investigation
Caffe Bene Boston – 333 Massachusetts Avenue Boston, MA 02115	☒	☒
Cast Iron Pot – 356 Bergen Boulevard Fairview, NJ 07022	☐	☒
BBQ Cliffside Park – 651 Anderson Avenue Cliffside Park, NJ 07010	☐	☒
Piccola Cucina Spring – 196 Spring Street New York, NY 10012	☐	☒
Global Kitchen – 52 W. 52nd Street New York, NY 10104	☐	☒
Caffe Bene MPD – 300 W. 17th Street New York, NY 10010	☐	☒
Caffe Bene 157th – 9 Edward Morgan Place New York, NY 10032	☐	☒

1.5 Executive Summary of Findings

Summary of environment reviewed	Each site reviewed by Foregenix consisted of one (1) or two (2) Point of Sale Terminals with the exception of the Global Kitchen location. This site included eight (8) Point of Sale systems. As part of the response process, Foregenix deployed our Incident Response technology *Serengeti* to all devices for ongoing monitoring during the duration of the investigation.
Was there conclusive evidence of breach?	☒ Yes ☐ No
If yes (There is conclusive evidence of breach), complete the following sections	

Date(s) of intrusion

The below table represents the dates of intrusions based on available *LogMeIn* log data provided by INNOAS, Inc..

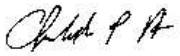
Location Name	D.B.A Name	Date of Intrusion
CB 17th Street LLC	Caffe Bene MPD	2016-12-10
House of Caffe Bene, Inc.	Caffe Bene 157th	2016-12-14
GKNY1 Inc.	Global Kitchen	2016-12-16
R & G Soho, LLC	Piccola Cucina Spring	2016-12-10
KEO BOO KEE Corp.	BBQ Cliffside Park	2016-12-13
Chen & Chen Brothers Inc.	Caffe Bene Boston	2016-12-10
Pinnacle Bar & Grill	Cast Iron Pot	2016-12-17
June & Shana, Inc.	Caffe Bene Sunnyside	2016-12-14
Lucky Star Caffe Inc.	Caffe Bene Brooklyn 18th	2016-12-10
Lee & Lim, LLC	BBQ Flushing	2016-12-09
725 Third Avenue Corp.	Bocca Bliss	2016-12-17
Jamo 26, Inc.	Izakaya Nomad	2016-12-10
R & G Soho, LLC	Piccola Cucina Prince	2016-12-17
Gogi, inc.	Soju Haus	2016-12-10
Pak Cafe Bene, LLC	Caffe Bene Jersey City	2016-12-15
Caffe Bene Fort Lee LLC	Caffe Bene Fort Lee	2016-12-14
Soonmyung Development Corp.	Caffe Bene New Brunswick	2016-12-14
Kenny Baek Corp.	BBQ Old Tappan	2016-12-15
Wally's Hot Bagels, LLC	Wally's	2016-12-17
BC of God	Boomboom Edison	2016-12-17
Namgung Corp.	Crome Fort Lee	2016-12-10
Casino Car Wash, Inc.	Casino Car Wash	2016-12-09
PHK Co, Inc.	Rokman	2016-12-09

	<table><tr><th>Location Name</th><th>D.B.A Name</th><th>Date of Intrusion</th></tr><tr><td>Classique I Dayspa, Inc.</td><td>Classique Day Spa</td><td>2016-12-15</td></tr><tr><td>Abies Corporation</td><td>Caffe Bene Ellicott City</td><td>2016-12-10</td></tr><tr><td>Caffe Bene Champaign Inc.</td><td>Caffe Bene Urbana</td><td>2016-12-13</td></tr><tr><td>Caffe Bene Midwest LLC.</td><td>Caffe Bene Glenview</td><td>2016-12-13</td></tr><tr><td>Caffe Bene Green Inc.</td><td>Caffe Bene Champaign</td><td>2016-12-10</td></tr><tr><td>KimcrystalMin Inc.</td><td>Caffe Bene Suwanee</td><td>2016-12-10</td></tr><tr><td>R & G Espanola, LLC</td><td>Piccola Cucina Miami</td><td>2016-12-10</td></tr><tr><td>Bae & Kim, Inc.</td><td>Caffe Bene Buena Park</td><td>2016-12-13</td></tr><tr><td>Nabee Inc.</td><td>Caffe Bene Western</td><td>2016-12-10</td></tr><tr><td>Kafferia, Inc.</td><td>Caffe Bene Wilshire</td><td>2016-12-14</td></tr><tr><td>JihoJiwoo, Inc.</td><td>Caffe Bene Rowland HTS</td><td>2016-12-10</td></tr><tr><td>MCKN Enterprise, Inc.</td><td>Caffe Bene San Diego</td><td>2016-12-09</td></tr><tr><td>San Marino Caffebene Inc.</td><td>Caffe Bene San Marino</td><td>2016-12-09</td></tr><tr><td>Carrot House Inc.</td><td>Caffe Bene Carrollton</td><td>2016-12-10</td></tr><tr><td>Caffe Bene Ktwon Inc.</td><td>Caffe Bene 32th</td><td>2016-12-15</td></tr><tr><td>Cibam Inc.</td><td>Caffe Bene Astoria</td><td>2016-12-15</td></tr></table>
Cause of the intrusion	The exact cause of the intrusion remains unknown to Foregenix; however, all indications suggest the service provider's LogMeIn credentials were somehow compromised. Attackers utilized the *LogMeIn* service installed on the remote Point of Sale systems to gain access to the various hosts and upon gaining access, malware was downloaded from the Internet via a .ZIP file. The .ZIP file contained three (3) executables that were used to install malware on the system and achieve persistence. (Please see Appendix D on page 53 for specific examples)
Has the breach been contained?	☒ Yes ☐ No
If yes, specify how the breach has been contained	The Point of Sale systems were re-imaged as part of the organisation's response to the breach. Unfortunately, the infected systems were re-imaged prior to forensic images of the systems were able to be captured for analysis.

Date of containment	2017-01 Foregenix estimates between mid to the end of January 2017 based on conversations with INNOAS
Is there evidence the cardholder data environment was breached?	☒ Yes – Please see the sites listed in Table 1 ☒ No
If no (There is no conclusive evidence of breach), complete the following sections	
Were system logs available for all relevant systems?	☐ Yes ☒ No
Were network logs available for all relevant systems?	☐ Yes ☒ No
Did the available logs provide the detail required by PCI DSS Requirement 10?	☐ Yes ☒ No
Were the log files in any way amended or tampered with prior to your investigation starting?	☒ Yes ☐ No
Were changed made to the environment prior to your investigation starting?	☒ Yes ☐ No
Was data pertaining to the breach deleted prior to your investigation starting?	☒ Yes ☐ No
Provide reasons why the evidence is inconclusive	All systems affected were re-imaged or replaced and software was reinstalled prior to the investigation commencing.

1.6 PFI Company Attestation of Independence

1. This investigation is being conducted strictly in accordance with all applicable requirements set forth in Section 2.3 of the *Qualification Requirements for PCI Forensic Investigators*, including but not limited to the requirements therein regarding independence, professional judgement, integrity, objectivity, impartiality and professional skepticism;
2. This PFI Preliminary Incident Response Report accurately identifies, describes, represents and characterises all of the factual evidence that the PFI Company and it's PFI Employees gathered, generated, discovered, reviewed and/or determined in their sole discretion to be relevant to this investigation in the course of performing the investigation; and
3. The judgements, conclusions and findings contained in this PFI Preliminary Incident Response Report (a) accurately reflect and are based solely upon the factual evidence described immediately above, (b) reflect the independent judgements, findings and conclusions of the PFI Company and its PFI Employees only, acting in their sole discretion, and (c) were not in any manner influenced, directed, controlled, modified, provided or subjected to any prior approval by the subject Entity Under Investigation, any contractor, representative, professional advisor, agent or affiliate thereof, or any other person or entity other that the PFI Company and its PFI Employees.

PFI Signature		**Date**	September 5th, 2017
PFI Name	Sterling Thomas	**Company**	Foregenix

2 Background

2.1 Background Information

Background			
Type of business entity	☐ Merchant (Brick & Mortar, eCommerce)	☐ Acquirer Processor	☐ Encryption Support Organisation (ESO)
	☐ Prepaid Issuer	☐ Issuer Processor	☒ Payment Application Vendor
	☐ Issuer	☐ ATM Processor	☐ Payment Application Reseller
	☐ Acquirer	☒ Third Party Service Provider (Identify type of Service Provider below)	
	Physical and logical management of Point of Sale systems on behalf of merchants.		
Number of Locations	No. of Locations	No. of Locations Assessed by PFI Company	
	62 The organisation provided services to merchants covering in excess of sixty physical locations. Due to the diversity of these locations and the fact that systems had been purged and re-imaged prior to Foregenix' involvement, it was agreed with the payment Brands that a sampling approach to the site analysis would be pursued. However, in order to ensure that the remaining sites were understood, Foregenix' Incident Response software *Serengeti* was deployed and used to assess as well as monitor the remaining devices for the duration of the investigation.	7 Pursuing a pre-approved sampling approach to the investigation of the dispersed environment, seven (7) locations were physically assessed during the course of this investigation. The remaining locations and systems were remotely assessed with the assistance of Foregenix' *Serengeti* solution.	
Parent Company (if applicable)	Not applicable – the organisation is a privately held company.		
Franchise of Corporate Owned	Not applicable – the organisation is a privately held company.		

3 Incident Dashboard

3.1 Summary

Summary			
Date when potential compromise was identified	In January 2017 several acquirers contacted INNOAS, Inc. to inform them that their merchant's may have sustained a data breach.		
Method of identification	☐ Self Detection	☐ Common Point of Purchase	☒ Other
If *other*, describe the method of identification	INNOAS, Inc. received notifications from several acquires that their customers may have sustained a card data compromise.		
Window of application, system or network vulnerability	Details of the "Window of Vulnerability" unfortunately cannot be clearly defined by Foregenix due to all the changes. Furthermore, as the means of compromised is believed to involve compromised credentials of a remote access facility, it is unclear how or when the security configuration of this remote access facility may have been vulnerable. As the Point of Sale devices were configured to *trust* this remote access mechanism the window of vulnerability could logically be defined as encompassing the period that the remote access facility has been in operation – early 2016 through 2017-01.		
Window of intrusion	2016-12-09 - 2017-01 Based on the evidence available, the Window of Intrusion has been defined as December 9th 2016, when the intruder first accessed the LogMeIn profile, through to January 2017 when INNOAS, Inc. became aware of the situation and began their remedial actions.		
Malware installation date(s), if applicable	2016-12-09 - 2017-12-17 This time-frame relating to the malware deployment is based on the remote access log details. Due to the clean-up operation that was evident, Foregenix has no ability, nor is it forensically possible to determine if malware was placed on a number of the merchant's systems.		
Date(s) of real time capture, if applicable	This information is unknown due to the the lack of available evidence for review. Hosts that had been compromised were re-imaged or decommissioned prior to any PFI firm involvement.		
Dates(s) that data was transferred out of the network, if applicable	This information is also unknown. Log evidence was not available for review for the time-frame noted in the Window of Intrusion due to logging configuration deficiencies. Logs could not be extracted that could conclusively determine how data was transferred from the merchant's environment. Additionally, system logs were either cleared, or deleted from the systems or unavailable due to system replacement or re-imaging.		
Window of payment card data storage	Based on forensic analysis of the merchant's systems, no evidence was found that the payment application was storing sensitive card-holder data as part of their normal operations.		
Transaction date(s) of stored accounts	No stored payment card data was identified within the environment(s) reviewed by Foregenix.		

3.2 Payment Application Information

Payment Application Details					
Payment Application Vendor	Korus Business, Inc. 22900 Shaw Rd. Sterling, VA 20166 (703) 574-5155				
Reseller / IT support that manages payment application / network	INNOAS, Inc. 21 Grand Avenue Suite 111 Palisades Park, NJ 07650 (201) 905-3521				
Payment Application Information	Payment Application Name	Version Number	Install Date	Last Patch Date	Application PA DSS Listed?
At the time of the breach	**JK Restaurant**	**1.00.0000**	**2017-05-25**	**N/A**	☐ Yes ☒ No
Current payment application	**No Changes to the merchants payment applications have been made.**				☐ Yes ☒ No

Software that stored CID, CAV2, CVC2, CVV2 or Track Data		
Name of Software	Version Number	Vendor Name
No changes have been made to the payment application(s). The application(s) were not storing sensitive card holder data.		

3.3 Payment Terminal Information

Payment Terminal Information	Product Name	Version Number	Install Date	Is Payment Terminal Listed?
At the time of the breach	N/A	N/A	N/A	☐ Yes ☐ No
Current Payment Terminal	N/A	N/A	N/A	☐ Yes ☐ No

3.4 Possible Exposure

Type of data exposed	☐ Cardholder Name	☐ Encrypted of Clear Text PINs	☒ PAN
	☐ Cardholder Address	☒ Expiry Date	☒ Track 2 Data
	☐ Track 1 Data	☐ CID, CAV2, CVC2, CVV2	☐ PIN Blocks
	☐ EMV Cryptograms		

Brand Exposure			
Brand	Brand Exposure	Number of Card Exposed	
		Malware Output Files	Inadvertent Storage
VISA	☐ Yes ☒ No	N/A	N/A
Mastercard	☐ Yes ☒ No	N/A	N/A
Discover	☐ Yes ☒ No	N/A	N/A
American Express	☐ Yes ☒ No	N/A	N/A
JCB	☐ Yes ☒ No	N/A	N/A
Other	☐ Yes ☒ No	N/A	N/A
If *other*, identify other brand exposure	INNOAS, Inc. is a service provider and does not process payment cards directly.		
Total number of cards exposed (both malware output file(s) and inadvertent storage)	This is unknown. Extensive clean-up was performed prior to Foregenix engagement as a PFI. INNOAS, Inc. replaced or re-imaged infected merchant's Point of Sale devices shortly after the discovery of malware.		
Is the above the total number of cards that are at risk?	☐ Yes ☒ No		
If *no*, explain	The extent of the at risk cards cannot be determined, primarily due to the extensive clean-up efforts that were undertaken prior to the engagement of Foregenix.		
Were cryptographic keys at risk?	☐ Yes ☒ No		
If *yes*, document the type of cryptographic keys at risk	Issuer Side Cryptographic Keys	Acquirer Side Cryptographic Keys	
	☐ Issuer Working keys (IWK)	☐ Acquirer Working Keys (AWK)	
	☐ PIN Verification Keys (PVK)	☐ POS, ATM, EPP PIN Encryption Keys	
	☐ PIN Generation Keys	☐ POS, ATM, EPP Key Encrypting Keys (KEKs)	
	☐ Master Derivation Keys (MDK)	☐ Remote Initialization KEYS	
	☐ Host to Host Working Keys	☐ Host to Host Working keys	
	☐ Key Encryption Keys (KEKs)	☐ Key Encryption Keys (KEKs)	
	☐ Switch Working Keys	☐ Switch Working Keys	
	☐ Other	☐ Point to Point Encryption Keys	
		☐ Other	

If *other* is indicated, describe	N/A	
Were Card Validation Codes or Values at risk?	☒ Yes ☐ No	
If yes, document the type of Card Validation Codes or Values at risk	Magnetic Stripe Based Security Features	Printed Security Features
	☐ CAV – Card Authentication Value (JCB Payment Cards)	☐ CAV2 – Card Authentication Value 2 (JCB Payment Cards)
	☒ CSC – Card Security Code (American Express)	☐ CID – Card Identification No. (American Express & Discover)
	☒ CVC – Card Validation Code (Mastercard Payment Cards)	☐ CVC2 – Card Validation Code 2 (Mastercard Payment Cards)
	☒ CVV – Card Verification Value (VISA & Discover Payment Cards)	☐ CVV2 – Card Verification Value 2 (VISA & Discover Payment Cards)

3.5 Incident Evidence and Cause Summary

Evidence Summary			
Logs that provided evidence	☐ Firewall Logs	☐ Web Server Logs	☐ Wireless Connection Logs
	☐ Transaction Logs	☐ Hardware Securing Module (HSM) Logs	☐ Anti Virus Logs
	☐ Database Queries	☐ File Integrity Monitoring Output	☒ Security Event Logs
	☐ FTP Server Logs	☐ Intrusion Detection Systems	☐ Network Device Logs
	☐ System Login Records	☒ Remote Access Logs	☐ Web Proxy Logs
Suspected cause summary and list of attack vectors	The exact cause of the intrusion is unknown to Foregenix, but as previously mentioned appears to involve the compromise of the service provider's remote access profile. Attackers utilized the *LogMeIn* service installed on the remote Point of Sale systems to gain access to the various hosts. Upon gaining access, malware was downloaded from the Internet in the form of a `.ZIP` file, which contained three (3) executable files that were used to install malware on the system and achieve persistence. (Please see Appendix D on page 53 for specific examples)		
If the initial attack vector is a phishing email (compromised account credentials), confirm that the phishing email, with headers and link has been included as an appendix to this report	N/A		
Is card data still at risk?	☐ Yes ☒ No		
If *yes*, describe the residual risk			

Law enforcement report date	Unknown
Law enforcement report case number	Unknown
Law enforcement contact name	Unknown
Law enforcement contact phone number	Unknown
If the case has not been reported to law enforcement, explain why	Foregenix advised INNOAS, Inc. that they are victim of a crime therefore should contact law enforcement. Foregenix is unaware ether the incident was pursued further with any local or federal law enforcement agencies.

4 Network Infrastructure Overview

4.1 Network Diagram(s)

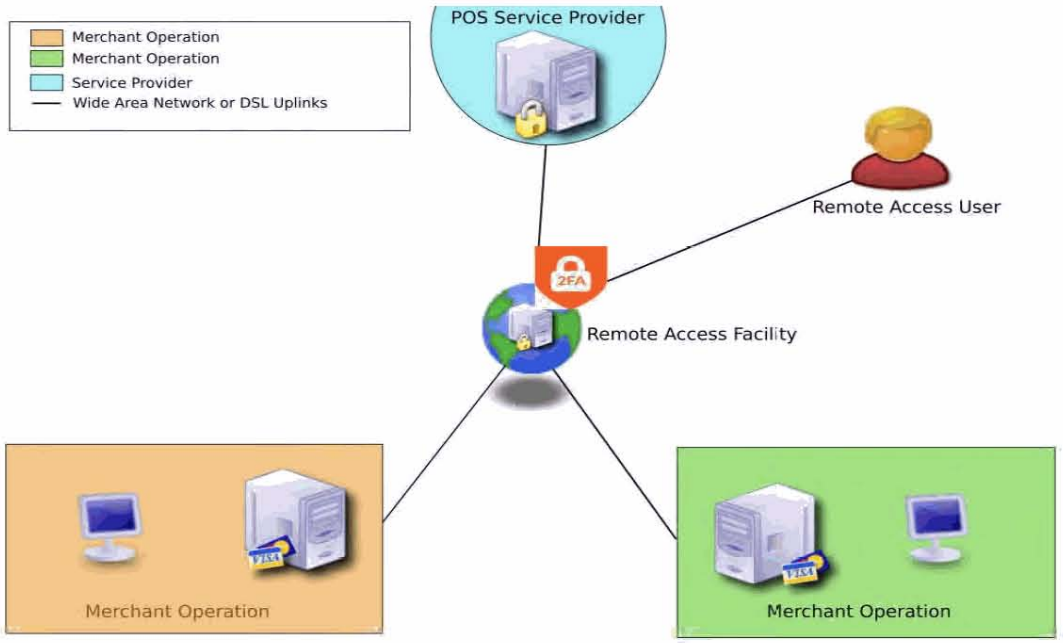


Illustration 1: High Level Network Topology

4.2 Infrastructure after the time-frame of the compromise

Infrastructure	
Were there any infrastructure components implemented or modified after the time-frame of the compromise?	Yes
If *yes*, describe.	All systems affected were re-imaged or replaced and software was reinstalled prior to the investigation commencing.

5 Findings

5.1 Third Party Payment Applications and Remote Access Applications

Payment Applications	
Identify any third party payment application(s), including version number	JK Restaurant Version 1.00.0000
Are there any upgrades / patches to the payment application(s) that address removal of magnetic stripe, card verification codes or values, and / or encrypted PIN blocks?	☐ Yes ☒ No
If yes, identify the payment application and the applicable upgrades / patches to the payment application that address removal of magnetic stripe data, card verification codes or values, and / or encrypted PIN blocks.	N/A
Identify remote access	*LogMeIn* *TeamViewer* *RealVNC* (INNOAS, Inc. Corporate)

5.2 Third Party Service Providers

Name of third party service provider	Purpose
Not applicable	Not applicable

5.3 Changes Made to the Entity Under Investigation's Computing Environment After the Identification of Compromise

Environmental Changes	
Payment Application	JK Restaurant
Reseller / IT support that manages the payment application / network	INNOAS, Inc.

Payment Application Information			
	Specific date of change	Version Number	Installation Date
At the time of the breach	No changes were made to the payment applications. Systems were re-imaged or replaced.		
Current payment application	No changes were made to the payment applications. Systems were re-imaged or replaced.		
Software that stored the CID, CAV2, CVC2, CVV2 or Track data			
	Name of Software	Version Number	Vendor Name
Software that stored the CID, CAV2, CVC2, CVV2 or Track data	N/A – The payment application(s) were not found to be storing sensitive card holder data.		

5.4 Timeline of Events

Date/Time Created	Activity	Description of Evidence	System / File Evidence
2016-12-09 through 2016-12-17	Malware Deployed	Katrina malware was deployed to multiple locations managed by INNOAS, Inc. through the service provider's LogMeIn profile.	Remote Access Logs
2017-01	Notification	INNOAS, Inc. receives notification from several acquirers of the potential of a data compromise for their merchants.	N/A
2017-01	Containment	Over a period of time prior to engaging Foregenix, INNOAS, Inc. reinstalled the Operating System and applications for Point of Sale systems affected by the malware.	N/A
2017-03-20	PFI Engaged	INNOAS, Inc. first contacts Foregenix and inquires about what a PFI investigation entails.	N/A
2017-04-20	PFI Engaged	INNOAS, Inc. re-engages with Foregenix. Amended proposal and contracts were provided.	N/A
2017-05-25	On-site Review	Prior to contracts being executed, Foregenix arrived onsite at Caffe Bene Boston 333 Massachusetts Avenue Boston, MA 02115 to physically inspect the environment and capture evidence. This event was to instruct INNOAS, Inc. on the process of collecting evidence. Evidence drives and tools were supplied to Jake Lee for the remaining full PFI sites	N/A
2017-05-25	Initial *Serengeti* Deployment	Initial deployment of the Serengeti solution is actioned at the outlet mentioned above	*Serengeti* Telemetry
2017-05-31	Contracts Executed	Contracts were officially executed.	N/A
2017-06-08	Reporting	Preliminary report issued to all parties	N/A
2017-06-08	Evidence Shipped	INNOAS, Inc. Ships evidence to the Forensic Laboratory	N/A

2017-06-12	Evidence Collecting	Evidence drives received from sampled locations and investigation commences	N/A
2017-06-12	Information Requested	Foregenix requests malware information from INNOAS, Inc.	N/A
2017-06-15	Status Update Call	First status update call scheduled with all relevant parties.	N/A
2017-06-15	Telemetry Provided	Telemetry data received from *Serengeti* was provided to INNOAS, Inc. for their attention and review.	N/A
2017-06-20	Information Requested	Foregenix sends 2nd request for the malware information to INNOAS, Inc.	N/A
2017-06-22	Status Update Call	Second status update call scheduled with all relevant parties.	N/A
2017-06-22	Information Requested	*LogMeIn* remote access logs requested for review.	N/A
2017-06-23	Malware Provided	Foregenix provided malware samples to all parties requesting the samples	N/A
2017-06-23	Information Received	*LogMeIn* remote access logs received for review.	N/A
2017-06-24	Information Requested	Foregenix requested eMail logs for review.	N/A
2017-08-10	Reporting	Final Report enters QA for review.	N/A
2017-09-05	Reporting	INNOAS, Inc. makes final payment and Final Report issued to all parties.	N/A

5.5 General Findings

Describe all relevant findings related to	
Firewalls	No logging available. Payment terminals are allowed direct access to the Internet.
Infrastructure	No centralized logging configured to retain logs.
Host	Passwords are not required for local authentication. No FIM (file integrity monitoring) is in place. A number of systems were discovered running out of date software and Operating Systems. Several hosts where observed to have unauthorized / unlicensed software installed.
Personnel	While personnel were forthcoming with the information, a better process needs to be in place to expedite incident requests.
Other	Remote access applications such as *LogMeIn* should utilized milti-factor authentication.
Identify specific dates related to the changes to the	
Network	No changes to the network have been noted.
System	All infected hosts identified by INNOAS, Inc. were re-imaged and redeployed to the merchant's locations

Payment Application	No changes to the payment applications were noted.
Personnel	None noted.
Other	None noted.

5.6 Unauthorised Access and / or Transfer of Data

Unauthorised Access or Data Transfer	
Identify any data accessed by unauthorised users(s)	The malware installed was capable of harvesting track data directly from process memory, exfiltrating the same information real time.
Identify any data transferred out of the network by unauthorised user(s)	No evidence was discovered to support data transfer out of the network. However, based on reverse engineering and publicly disclosed write-ups of the malware family of the malware installed, data exfiltration takes place over POST requests over plain HTTP requests.
Identify any evidence of data deletion from systems involved in the compromise	During the forensic processing, positive hits for the malware and suspect malicious IP address were found. These fragments were located in unallocated space and file slack of the disk. The anti-forensic tool *CCleaner* was also used as part of the INNOAS, Inc.reinstallation process, therefore making recovery of these files not viable.
Was any deleted data recovered through forensic file recovery methods?	☐ Yes ☒ No
If yes, describe what deleted data was recovered	N/A

5.7 Compromised Systems / Hosts

Confirmed Evidence of Compromise	
Identified Compromised Sites	Functionality of System or Host
Caffe Bene MPD	Point of Sale Terminal
Caffe Bene 157th	Point of Sale Terminal
Global Kitchen	Point of Sale Terminal
Piccola Cucina Spring	Point of Sale Terminal
BBQ Cliffside Park	Point of Sale Terminal
Caffe Bene Boston	Point of Sale Terminal
Cast Iron Pot	Point of Sale Terminal

Confirmed Evidence of Compromise	
Identified Compromised Sites	Functionality of System or Host
Caffe Bene Sunnyside	Point of Sale Terminal
Caffe Bene Brooklyn 18th	Point of Sale Terminal
BBQ Flushing	Point of Sale Terminal
Bocca Bliss	Point of Sale Terminal
Izakaya Nomad	Point of Sale Terminal
Piccola Cucina Prince	Point of Sale Terminal
Soju Haus	Point of Sale Terminal
Caffe Bene Jersey City	Point of Sale Terminal
Caffe Bene Fort Lee	Point of Sale Terminal
Caffe Bene New Brunswick	Point of Sale Terminal
BBQ Old Tappan	Point of Sale Terminal
Wally's	Point of Sale Terminal
Boomboom Edison	Point of Sale Terminal
Crome Fort Lee	Point of Sale Terminal
Casino Car Wash	Point of Sale Terminal
Rokman	Point of Sale Terminal
Classique Day Spa	Point of Sale Terminal
Caffe Bene Ellicott City	Point of Sale Terminal
Caffe Bene Urbana	Point of Sale Terminal
Caffe Bene Glenview	Point of Sale Terminal
Caffe Bene Champaign	Point of Sale Terminal
Caffe Bene Suwanee	Point of Sale Terminal
Piccola Cucina Miami	Point of Sale Terminal

Confirmed Evidence of Compromise	
Identified Compromised Sites	Functionality of System or Host
Caffe Bene Buena Park	Point of Sale Terminal
Caffe Bene Western	Point of Sale Terminal
Caffe Bene Wilshire	Point of Sale Terminal
Caffe Bene Rowland HTS	Point of Sale Terminal
Caffe Bene San Diego	Point of Sale Terminal
Caffe Bene San Marino	Point of Sale Terminal
Caffe Bene Carrollton	Point of Sale Terminal
Caffe Bene 32th	Point of Sale Terminal
Caffe Bene Astoria	Point of Sale Terminal

5.8 No Conclusive Evidence of Breach

Provide detailed analysis and feedback regarding the inconclusive case	The evidence collected by Foregenix was from systems that had been completely reinstalled after the malware infection was discovered. The full Operating System and applications were rebuilt on these machines prior to Foregenix being engaged for the investigation, resulting in most evidence of the compromise being destroyed. Only a single system (`GK_POS_SERVER`) from Global Kitchen contained any evidence of the malware. These findings are based on several forensic and forensic processing techniques, including, but not limited to the following: • Memory Analysis - Active RAM (Random Access Memory) was analysed for the presence of malware or artefacts indicating it's operation. Analysis for this data included searching for hooks into the payment application which malware often targets to capture sensitive data. No hooks or injected DLL's were observed. No malware , or indications of compromise have been detected. • Volatile Data Analysis - Volatile information such as active network connections, running processes and open ports/files were analysed. System monitoring utilities had been run to observe the system state. Active processes and network connections were monitored. No new processes or connections had been detected. • Hash Analysis (MD5, SHA1 and Fuzzy Hashes) - Hashes of the files systems where acquired and processed for known malicious content which yielded a negative result. • File System Analysis - No unknown binary files have been detected, including batch files or scripts used for malicious intent. • Service / Registry Analysis - No unknown service entries have been added. • Timeline Analysis - The file system was reviewed in a chronological event format. While file system data changes by the millisecond, a review of the systems for the alleged time-frame did not conclude any positive findings of compromise. • $MFT (Master File Table) Analysis. The Master File Table was analysed for signs of time stomping. Attackers often change time stamps on malicious files placed on compromised servers to throw off investigative processes. No indications that file time manipulation was observed during the investigation. • Keyword Searching, including data patterns for Card Holder Data (PAN, Track I, and Track II). This also included searching for obfuscated forms of card holder data associated with card parsing malware as well as various patterns for malware and attack tools. • Virus Analysis: No known viruses have been detected. A review of the Anti-Virus logs in addition to separate scans completed by Foregenix. • Event Log Analysis: No suspicious signs of invalid logins or invalid/rouge process executions. Foregenix has also deployed our Incident Response technology *Serengeti* on numerous systems beginning on May 25th, 2017. During the monitoring phase no indications of malicious activity has been detected to date.
Provide the PFI Company's opinion as to the reason for the forensic investigation being inconclusive	Much of the evidence necessary to draw definitive conclusions about the attack was destroyed in the process of re-imaging the systems performed by INNOAS, Inc..

6 Containment Plan for the Entity Under Investigation

6.1 Containment Actions Completed

Containment Action Completed	Date(s) of Containment
INNOAS, Inc. re-imaged and or redeployed new Point of Sale systems to all infected hosts.	January 2017
TeamViewer remote access software replaced *LogMeIn*.	January 2017

6.2 Containment Actions Planned

Containment Action Planned	Planned Date(s) of Containment
None at this time.	N/A

7 Recommendations

7.1 Recommendations for the Entity

Recommendations	Priority Ranking
All remote access into the cardholder data environment must use multi-factor authentication. Multi-factor authentication is normally defined as an authentication method requiring at least something a user knows (password) and something the user has in their possession (token, certificate).	1
Passwords on the compromised systems and any systems *visible* to the compromised machines must be changed. This includes system passwords, but also remote connectivity, applications, services and any websites accessed via these machines. Ensure strong passwords are used.	2
Patching and upgrade procedures should be reviewed and updated in order to ensure that there are no systems within the cardholder data environment that are left unpatched and/or running out of date software.	3
System configuration standards should be developed and applied to all systems within the cardholder data environment in accordance with all requirements in the PCI DSS section 2.	4
Deploy / enable File-Integrity Monitoring (FIM) software capable of detecting and alerting on modifications, additions or removal of critical files which impact the security of the system(s) within the card-holder environment.	5
While logging is just one aspect of security. To be of value, audit logs will need to be reviewed on a regular basis to identify security incidents and potential weaknesses in the security structure. This can be done with the use of monitoring software or other utilities for this purpose. A process should be developed, either in-house or outsourced for reviewing logs and alerts. Logs need to be easily searched and exportable in the event of a security incident. Ensure that any logging solution implemented complies with all the requirements in Section 10 of the PCI DSS.	6
Foregenix has identified recommendations for each component of an Incident Response Plan which are outlined below. These recommendations will serve as a guide in formalizing an Incident Response Plan. 1. Establish an Incident Response Oversight Committee (this function can be integrated with any existing committees) for strategic management to ensure alignment with business objectives of the organization. 2. Establish an Incident Response Auditing Team to audit the operational procedures to ascertain whether results are consistent with established objectives and goals and whether the procedures are carried out as planned. 3. Revise the existing team structure to: ◦ Ensure clarity of roles and responsibilities ◦ Ensure accountability for assigned responsibilities 4. Develop an Incident Response Plan to ensure the following (at a minimum): ◦ Ease of understanding ◦ Proper categorization of major components of the plan ◦ User friendliness	7

◦ Simplification of the team structure and assigned roles and responsibilities. ◦ Inclusion and integration of the key components of an effective Incident Response Plan e.g. communication plan, notification forms etc. ◦ Elimination of unnecessary text to facilitate review in a timely manner during the occurrence of an incident for guidance 5. Development of matrices and flow charts to aid visual understanding of process flow.-Incident Response Plan to include detailed procedures and process flow charts for: ◦ Detection ◦ Assessment and notification ◦ Communication ◦ Forensics ◦ Containment and Mitigation ◦ Documentation ◦ Lessons Learned 6. Identify existing resource requirements (both in terms of forensic tools and personnel) for forensic data gathering and analysis. Ensure availability of trained forensic staff on the Incident Response Team to facilitate timely data gathering and preservation of evidence while the outsourced virtual forensic team is activated. Ensure contractual agreement(s) with vendors that provide forensic services to serve as a virtual team member on the Incident Response Team. 7. Require documentation of all incident activities from detection to lessons learned meeting as a standard procedure. 8. Re-evaluate the existing training program to develop customized training for the various identified team members based on roles and responsibilities. Develop a framework for hands-on and in person training program for key team members of the Incident Response Plan. 9. Update the Incident Response Policy and Plan to include testing of the plan on a regular basis (at least annually, preferably twice a year). Establish a process to utilize the information accumulated from the Lessons Learned Meeting to identify systemic security weaknesses and deficiencies in the policies and procedures.	

7.2 Other Recommendations of Comments

Additional Comments	
Other recommendations or comments form the PFI Company	Network segmentation should be considered to limit the risk of systems not in the payment environment communicating with the systems that process card holder data. The use of a P2PE solution should be considered to limit the risk of card exposure to Point of Sale systems that have been compromised.

Appendix A: PCI DSS Overview

A.1 PCI DSS Summary

Incident Overview		
Type of Business Entity	☐ Merchant (Brick & Mortar, eCommerce etc)	☐ ATM Processor
	☐ Prepaid Issuer	☒ Third Party Service Provider
	☐ Issuer	☐ Encryption Support Organisation
	☐ Issuer Processor	☐ Payment Application Vendor
	☐ Acquirer	☐ Payment Application Reseller
	☐ Acquirer Processor	☐ Other
	Describe: The investigated entity is a service provider that provides hardware and software support for POS systems to it's clients. The services provided include full hardware support as well as installation and updates to software run by the POS systems at their clients' locations.	
Summary statement for findings, including factors that caused or contributed to the breach. (For example, memory-scraping malware, remote access, SQL injection, etc.)	The exact cause of the intrusion is unknown to Foregenix; however, based on current evidence it appears to have involved the compromise of the service provider's remote access profile. Attackers utilized the *LogMeIn* service installed on the remote Point of Sale systems to gain access to the various hosts. Upon gaining access, malware was downloaded from the Internet in the form of a `.ZIP` file which contained three (3) executables that were used to install malware on the system and achieve persistence.	
Indicate the version of the PCI DSS used for this part of the investigation.	PCI DSS v3.2 was used to assess the compliance posture of this merchant's environment.	
Did the entity utilize any advanced payment technology at the time of the compromise— e.g., end-to-end encryption or tokenisation?	☐ YES ☒ NO	
If yes, provide details of the product/solution in use.	Not applicable	

A.2 PCI DSS Overview

PCI DSS Requirement	Requirement Fully Assessed?	In Place	Cause of Breach	Contributory to Breach	Findings
Build & Maintain s Secure Firewall					
Requirement 1: **Install and maintain a firewall configuration to protect card holder data**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☒ Yes ☐ No ☐ Unknown	1.1.2 – 1.1.3 - No network or data flow diagrams were available for review. 1.2 -There are no router or firewall rules restricting traffic into the cardholder data environment (CDE) from the internal, untrusted network. 1.3.4 – There were no anti-spoofing measures to detect and block forged source IP addresses. 1.3.6 – There was no stateful inspection (dynamic packet filtering) operational. 1.4 - 1.5 - Was not assessed for this requirement. It should be noted, that several locations were observed to have public wifi on the same network as the Point of Sale devices
Requirement 2: **Do not use vendor-supplied defaults for system password and other security parameters**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☐ No ☒ Unknown	☒ Yes ☐ No ☐ Unknown	2.2 – Configuration standards were no tin place for CDE systems. Local account passwords are not required Requirement 2.5 was not assessed.
Protect Cardholder Data					
Requirement 3: **Protect stored card holder data**	☐ Yes ☒ No	☐ Yes ☒ Partial Yes ☐ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☐ Yes ☒ No ☐ Unknown	Forensic analysis conducted by Foregenix of the sample set of Point of Sale systems, which included affected hosts indicated that the payment application(s) WAS NOT storing sensitive card holder data in the clear.
Requirement 4: **Encrypt transmission of card holder data across open, public networks**	☐ Yes ☒ No	☐ Yes ☒ Partial Yes ☐ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☐ Yes ☒ No ☐ Unknown	Based on the architecture and payment applications, Foregenix found no indications that sensitive card holder data would be sent out over public networks in an unencrypted format.
Maintain a Vulnerability Management Program					
Requirement 5: **Use and regularly update Anti-Virus software programs**	☐ Yes ☒ No	☐ Yes ☒ Partial Yes ☐ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☒ Yes ☐ No ☐ Unknown	Anti-virus WAS in place on all systems for Point ofSale end points, however was not locked down to prevent unauthorized changes, such as disabling of the controls. Logging for the Anti-virus did not comply with Requirement 10.2, however.

PCI DSS Requirement	Requirement Fully Assessed?	In Place	Cause of Breach	Contributory to Breach	Findings
Requirement 6: **Develop and maintain secure systems and applications**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☐ No ☒ Not Assessed	☐ Yes ☐ No ☒ Unknown	☐ Yes ☐ No ☒ Unknown	This requirement was not assessed. No payment applications are developed by the service provider.
Implement Strong Access Control Measures					
Requirement 7: **Restrict access to card holder data by business need-to-know**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☐ No ☒ Unknown	☐ Yes ☐ No ☒ Unknown	7.1 – 7.2.3 – Users do not have the ability to view card holder data. 7.3 - Security policy was not assessed for this requirement.
Requirement 8: **Assign a unique ID to each person with computer access**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☒ Yes ☐ No ☐ Unknown	☒ Yes ☐ No ☐ Unknown	8.5 - Is not in place. The system(s) contained several generic id's which were enabled. 8.8 - Security policy was not assessed for this requirement
Requirement 9: **Restrict physical access to card holder data**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☐ No ☒ Not Assessed	☐ Yes ☐ No ☒ Unknown	☐ Yes ☐ No ☒ Unknown	This requirement was not assessed.
Regularly Monitor and Test Networks					
Requirement 10: **Track and monitor all access to network resources and card holder data**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☒ Yes ☐ No ☐ Unknown	10.1 – 10.3 - Are not in place. Audit logging was limited. Security logs where not available for all systems for the time-frame. 10.5.4 – Centralized logging was not in place. 10.6 – 10.7 - Are not in place.
Requirement 11: **Regularly test security systems and processes**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☒ Yes ☐ No ☐ Unknown	11.1 – 11.5.1 Are not in place. No regular security testing was being performed. No File Integrity Monitoring (FIM) was in place at the time of the incident. 11.6 – Security policy was not assessed for this requirement.
Maintain an Information Security Policy					

PCI DSS Requirement	Requirement Fully Assessed?	In Place	Cause of Breach	Contributory to Breach	Findings
Requirement 12: **Maintain a policy that addresses information security for employees and contractors**	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☐ No ☒ Not Assessed	☐ Yes ☒ No ☐ Unknown	☐ Yes ☒ No ☐ Unknown	This requirement was not assessed.

Appendix B: Threat Indicator Information

B.1 Threat Indicator Summary

Indicator File	Indicator Type	Date / Time	Action / Kill Chain
Description: File dropper which also reads remote access related keys. The malware makes a connection to `146.0.77.88` on TCP Port `9090`	Application	Unknown	Exploitation, Exfiltration
	Filename	Description / File Type	File Size
	`artifact.exe`	Executable	97 kB
	Hash Type / Value	IP Addresses	Registry Settings
	`md5:a2a160f767829dc70bb584b46ee11c9e`	`146.0.77.88`	N/A
	Domain	Domain Time of Lookup	System Path
	N/A	N/A	various
	Target eMail Addresses	Additional Information	
	N/A	N/A	

Table 2: Malware `artifact.exe`

Indicator File	Indicator Type	Date / Time	Action / Kill Chain
Description: Unknown binary file. The binary appears to be a file extractor when executed.	Application	Unknown	Exploitation
	Filename	Description / File Type	File Size
	`v5.exe`	Executable	`146 kB`
	Hash Type / Value	IP Addresses	Registry Settings
	`md5:928723bdbd90c3dc82879bb6d505fc2f`	N/A	N/A
	Domain	Domain Time of Lookup	System Path
	N/A	N/A	various
	Target eMail Addresses	Additional Information	
	N/A	Extracts the following when executed: Filepath %APPDATA%\V1hAY0cx\osfip.exe Size 146KiB (149171 bytes) Filepath %TEMP%\palletizations.dll Size 76KiB (77824 bytes) Filepath %TEMP%\nsh77B6.tmp\System.dll Size 11KiB (11264 bytes) Filepath %TEMP%\BUTTON.HTM Size 5.2KiB (5274 bytes) Filepath %TEMP%\Sultana.hiYU Size 70KiB (72090 bytes)	

Table 3: Malware `v5.exe`

Indicator File	Indicator Type	Date / Time	Action / Kill Chain
Description: This file is part of the *Alina.POS* malware family. The file makes a connection to `103.193.4.121` on TCP Port `80`.	Application	Unknown	Exploitation
	Filename	Description / File Type	File Size
	`rfv.exe`	Executable	`446 kB`
	Hash Type / Value	IP Addresses	Registry Settings

	`md5:366d954fb29fffe8bb280303032fa94b`	`103.193.4.121`	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchost]`
			
			`Data = "%APPDATA %\Roaming\usercache\svchost.exe"`

	Domain	Domain Time of Lookup	System Path
	pyssh.com	N/A	various
	Target eMail Addresses	Additional Information	
	N/A	`POST /rfvrfv/settings.php HTTP/1.1 Accept: application/octet-stream Content-Type: application/octet-stream Connection: Close User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0 Host: pyssh.com Content-Length: 82 Cache-Control: no-cache 666 OK`	

Table 4: Malware `rfv.exe`

Indicator File	Indicator Type	Date / Time	Action / Kill Chain
Description: This file is part of the *Alina.POS* malware family. The file makes a connection to `103.193.4.121` on TCP Port `80`.	Application	Unknown	Exploitation, Exfiltration
	Filename	Description / File Type	File Size
	`svchost.exe`	Executable	`446 kB`
	Hash Type / Value	IP Addresses	Registry Settings
	`md5:366d954fb29fffe8bb280303032fa94b`	`103.193.4.121`	`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchost]` `Data = "%APPDATA %\Roaming\usercache\svchost.exe"`
	Domain	Domain Time of Lookup	System Path
	pyssh.com	N/A	`%APPDATA%\Roaming\usercache\svchost.exe`
	Target eMail Addresses	Additional Information	
	N/A	`POST /rfvrfv/settings.php HTTP/1.1 Accept: application/octet-stream Content-Type: application/octet-stream Connection: Close User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0 Host: pyssh.com Content-Length: 82 Cache-Control: no-cache 666 OK`	

Table 5: Malware `svchost.exe`

Appendix C: Impacted Entities

NOTE: This information was provided various parties such as listed acquirers and or card brands.

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
Carrot House Inc.	Carrollton	TX		Unknown	Unknown	N/A	000008023858155 5179248901126670 0008023858155 5179248901126670 0008023858155 5179248901126670 0008023858155 517924890112667	First Data (EMV Insert Terminal)	2016-12-10	January 2017
Moonstone Nail & Spa	Frisco	TX	75034	Unknown	Unknown	N/A	554402004104956	Elavon	Unknown	Unknown
Anlaur, Inc.	Berwyn	PA		Unknown	Unknown	N/A	413600541204112 000008029163568 413600541204112 000008029163568 413600541204112 000008029163568 413600541204112 000008029163568	POS Maintenance Only	Unknown	Unknown
29 Iris Nail and Spa, Inc.	Lansdale	PA		Unknown	Unknown	N/A	000008027737611 517924890113913 000008027737611 517924890113913 000008027737611 517924890113913 000008027737611 517924890113913	First Data (EMV Insert Terminal)	Unknown	Unknown

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
House of Caffe Bene, Inc.	New York	NY	10032	OPTBLUE	601113015978177	N/A	8027341588	Elavon (Magnetic Swipe)	2016-12-14	January 2017
Caffe Bene Ktwon Inc.	New York	NY	10001	OPTBLUE	601113016066386	N/A	8027434847	Elavon (EMV Insert Terminal)	2016-12-15	January 2017
Cibam Inc.	Astoria	NY	11103	OPTBLUE	601113016082862	N/A	8027455016	Elavon (Magnetic Swipe)	2016-12-15	January 2017
June & Shana, Inc.	Sunnyside	NY	11104	OPTBLUE	601113015616371	N/A	8026947294 11220060873388480 26947294 11220060873388480 26947294 11220060873388480 26947294 112200608733884	Elavon (Magnetic Swipe)	2016-12-14	January 2017
CB 17th Street LLC	New York	NY	10010	OPTBLUE	601113016949482	N/A	8028435769	Elavon (Magnetic Swipe)	2016-12-10	January 2017
Lucky Star Caffe Inc.	Brooklyn	NY	11204	OPTBLUE	601113017102339	N/A	8028609009	Elavon (Magnetic Swipe)	2016-12-10	January 2017
Lee & Lim, LLC	Flushing	NY	11358	OPTBLUE	601113009166847	N/A	8015399754 51792489011261880 15399754 51792489011261880 15399754 51792489011261880	Elavon (Magnetic Swipe)	2016-12-09	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
							15399754 517924890112618			
BBQ Chicken Little Neck Corp.	Little Neck	NY		Unknown	Unknown	N/A	118100001180001 517924890112329 118100001180001 517924890112329 118100001180001 517924890112329 118100001180001 517924890112329	First Data (EMV Insert Terminal)	Unknown	Unknown
725 Third Avenue Corp.	New York	NY	10017	OPTBLUE	601113016227483	N/A	8027607475	Elavon (Magnetic Swipe)	2016-12-17	January 2017
GKNY1 Inc.	New York	NY	10104	Unknown	Unknown	N/A	000849279171888 517924890112352 004445021769794 000520001143579 520001143579000 000849279171888 517924890112352 004445021769794 000520001143579 520001143579000 000849279171888 517924890112352 004445021769794 000520001143579 520001143579000 000849279171888	First Data (Magnetic Swipe)	2016-12-16	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
							517924890112352 004445021769794 000520001143579 520001143579000			
Jamo 26, Inc.	New York	NY		Unknown	Unknown	N/A	000008027052979 517924890113152 000008027052979 517924890113152 000008027052979 517924890113152	First Data (EMV Insert Terminal)	2016-12-10	January 2017
R & G Soho, LLC	New York	NY		Unknown	Unknown	N/A	588167401501640 000008023081238 588167401501640 000008023081238 588167401501640 000008023081238	Chase Paymentech (Magnetic Swipe)	2016-12-10	January 2017
R & G Soho, LLC	New York	NY		Unknown	Unknown	N/A	720000376020001 720000376020003 720000376020001 720000376020003 720000376020001 720000376020003	Chase Paymentech (Magnetic Swipe)	2016-12-17	January 2017
Gogi, inc.	New York	NY	10016	OPTBLUE	601113014771581	N/A	8024025143 00000803109066880 24025143 00000803109066880 24025143 000008031090668	Elavon (Magnetic Swipe)	2016-12-10	January 2017
Amber Nail & Spa, Inc	Bronx	NY	10461	OPTBLUE	601113017016216	N/A	8028510181	Elavon	Unknown	Unknown

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
								(Magnetic Swipe)		
Blooming Nail and Foot Spa Inc.	White Plains	NY	10601	OPTBLUE	601113014887007	N/A	8024130570	Elavon Merrick Bank	Unknown	Unknown
Gel Factory Corp.	East Northport	NY		Unknown	Unknown	N/A	517924890112253	First Data (EMV Insert Terminal)	Unknown	Unknown
Peggie Nail Inc.	New York	NY	10016	OPTBLUE	601113018613649	N/A	8030308814	Elavon (Magnetic Swipe)	Unknown	Unknown
Town Nail & Foot Spa Inc.	Scarsdale	NY		Unknown	Unknown	N/A	8024070909	POS Maintenance Only	Unknown	Unknown
Samhyungjae Corp.	New York	NY	10001	OPTBLUE	601113014608676	N/A	8023849030	Elavon (Magnetic Swipe)	Unknown	Unknown
Damoa Union Inc.	Flushing	NY	11354	OPTBLUE	601113017628002	N/A	8029193029	Elavon (EMV Insert Terminal-no POS transaction)	Unknown	Unknown
Pak Cafe Bene, LLC	Jersey City	NJ		OPTBLUE	601113017012330	N/A	8028505769	Elavon (Magnetic Swipe)	2016-12-15	January 2017
Caffe Bene Fort Lee LLC	Fort Lee	NJ		Unknown	Unknown	N/A	000008024090378 517924890112725 000008024090378 517924890112725 000008024090378	First Data (EMV Insert Terminal)	2016-12-14	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
							517924890112725			
Soonmyung Development Corp.	NEW BRUNSWICK	NJ		Unknown	Unknown	N/A	000483227621990 413600070401036 000483227621990 413600070401036 000483227621990 413600070401036	Elavon (Magnetic Swipe)	2016-12-14	January 2017
KEO BOO KEE Corp.	Cliffside Park	NJ		Unknown	Unknown	N/A	517924890113509	First Data (EMV Insert Terminal)	2016-12-13	January 2017
Kenny Baek Corp.	Old Tappan	NJ		Unknown	Unknown	N/A	517924890111222 118100001218001 517924890111222 118100001218001 517924890111222 118100001218001	First Data (EMV Insert Terminal)	2016-12-15	January 2017
Pinnacle Bar & Grill	Fairview	NJ		Unknown	Unknown	N/A	334400273668884	Bankcard Service Merrick Bank (EMV Insert Terminal)	2016-12-17	January 2017
Wally's Hot Bagels, LLC	Closter	NJ		Unknown	Unknown	N/A	372361901880	First Data (Magnetic Swipe)	2016-12-17	January 2017
Taste Treat LLC	Rutherford	NJ		Unknown	Unknown	N/A	000008023885182 517924890112774 000008023885182 517924890112774	First Data (EMV Insert Terminal)	Unknown	Unknown
BC of God	Edison	NJ		Unknown	Unknown	N/A	517924890113996	First Data	2016-12-17	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
							000008024239207 517924890113996 000008024239207	(EMV Insert Terminal)		
Namgung Corp.	Fort Lee	NJ		Unknown	Unknown	N/A	518089730633674 518089730633732 518089730633674 518089730633732	POS Maintenance Only	2016-12-10	January 2017
Spoon & Chopstick LLC	Palisades Park	NJ		OPTBLUE	601113016329818	N/A	8027730335	Elavon (Magnetic Swipe)	Unknown	Unknown
Spa Reee Inc.	Gillette	NJ		ONE POINT	601113015721874	N/A	8027278608	Elavon (EMV Insert Terminal-no POS transaction)	Unknown	Unknown
J & J Bloom Spa, Inc	Springfield	NJ		Unknown	Unknown	N/A	000008029743690 517924890112873 797900665851396 000008029743690 517924890112873 797900665851396	First Data (EMV Insert Terminal)	Unknown	Unknown
Casino Car Wash, Inc.	Palisades Park	NJ		OPTBLUE	601113016695218	N/A	8028151408	Elavon (Magnetic Swipe)	2016-12-09	January 2017
PHK Co, Inc.	Palisades Park	NJ		Unknown	Unknown	N/A	000008029534198 51792489011112300 0008029534198 517924890111123	First Data / Elavon (both EMV Insert Terminal)	2016-12-09	January 2017
Classique I Dayspa, Inc.	Waldwick	NJ		Unknown	Unknown	N/A	518089294713110	POS	2016-12-15	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
								Maintenance Only		
J Beauty Spa Corp.	Jersey City	NJ		OPTBLUE	601113015481313	N/A	8026801871	Elavon	Unknown	Unknown
Dream Nail & Spa, Inc	Jersey City	NJ		Unknown	Unknown	N/A	517924890111115 118100001591001 517924890111115 118100001591001	First Data (EMV Insert Terminal)	Unknown	Unknown
Ohnas Corp.	Bedminster	NJ		Unknown	Unknown	N/A	518089731202263	POS Maintenance Only	Unknown	Unknown
Bloom Spa, Inc.	Hoboken	NJ		Unknown	Unknown	N/A	000008028781345 008788270093926 517924890112733 000008028781345 008788270093926 517924890112733	First Data (EMV Insert Terminal)	Unknown	Unknown
Lemoine Gateaux Bakery LLC	Fort Lee	NJ		OPTBLUE	601113017277107	N/A	8028802117 06000003926900180 28802117 060000039269001	Elavon (Magnetic Swipe)	Unknown	Unknown
Gateaux Bakery Corp.	Closter	NJ		Unknown	Unknown	N/A	517924890103708	First Data	Unknown	Unknown
TLJ Ridgefield Inc.	Ridgefield	NJ		Unknown	Unknown	N/A	517924890103666	First Data	Unknown	Unknown
Café Nomis Inc.	Bayonne	NJ		OPTBLUE	601113017604862	N/A	8029163816	Elavon (Magnetic Swipe)	Unknown	Unknown
Abies Corporation	Ellicott City	MD	21042	OPTBLUE	601113016541479	N/A	8027976342	Elavon (Magnetic	2016-12-10	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
								Swipe)		
Chen & Chen Brothers Inc.	Boston	MA		OPTBLUE	601113015997250	N/A	8027364317	Elavon (Magnetic Swipe)	2016-12-10	January 2017
Caffe Bene Champaign Inc.	Urbana	IL	61801	OPTBLUE	601113015528345	N/A	8026856594	Elavon (Magnetic Swipe)	2016-12-13	January 2017
Caffe Bene Midwest LLC.	Glenview	IL	60025	OPTBLUE	601113015579561	N/A	8026903750	Elavon (Magnetic Swipe)	2016-12-13	January 2017
Caffe Bene Green Inc.	Champaign	IL	61820	OPTBLUE	601113017464283	N/A	8029007757	Elavon (Magnetic Swipe)	2016-12-10	January 2017
KimcrystalMin Inc.	Macon	GA	31220	Not applicable	601113017012439	N/A	8028505868 554402004101952	Elavon (no POS Transaction)	2016-12-10	January 2017
R & G Espanola, LLC	Miami Beach	FL		Unknown	Unknown	N/A	8023081196	POS Maintenance Only	2016-12-10	January 2017
Bae & Kim, Inc.	Buena Park	CA	90621	OPTBLUE	601113016355995	N/A	8027759011	Elavon (Magnetic Swipe)	2016-12-13	January 2017
Nabee Inc.	Los Angeles	CA		Unknown	Unknown	N/A	118100001562001	First Data (EMV Insert Terminal)	2016-12-10	January 2017
Kafferia, Inc.	Los Angeles	CA	90010	OPTBLUE	601113016383062	N/A	8027789729	Elavon (Magnetic Swipe)	2016-12-14	January 2017
JihoJiwoo, Inc.	Rowland	CA	91748	OPTBLUE	601113016837562	N/A	8028310129	Elavon	2016-12-10	January 2017

Merchant Name	Merchant Address			Merchant Identification Number				Acquirer Name	At Risk Timeframe	
	City	State	Zip	American Exp.	Discover	JCB Int.	Mastercard/VISA		Start Date	End Date
	Heights							(Magnetic Swipe)		
MCKN Enterprise, Inc.	Sandiego	CA	92111	OPTBLUE	601113017309900	N/A	8028837923	Elavon (Magnetic Swipe)	2016-12-09	January 2017
San Marino Caffebene Inc.	San Marino	CA	91108	OPTBLUE	601113017230551	N/A	8028748641	Elavon (Magnetic Swipe)	2016-12-09	January 2017

Appendix D: List of Attack Vectors / Intrusion Root Causes / Contributing Factors

Vector Type	Specifics
Host	☒ Host – Auto login enabled
	☒ Host – Local accounts are default/unsecured
	☐ Host – Local accounts have weak passwords
	☒ Host – No/limited system hardening
	☒ Host – No/limited system logging
	☐ Host – System allows insecure remote access
	☐ Host – System contains PAN/track data
	☒ Host – System has unrestricted network/Internet access
	☐ Host – System interfaces with POS environment
	☐ Host – System lacks anti-virus/anti-malware/HIPS
	☐ Host – System not inventoried/accounted
	☐ Host – System not patched/maintained
	☐ Host – System runs high-risk/insecure applications
	☒ Host – System runs non-standard/proprietary software
	☐ Host – System used for personal reasons

Vector Type	Specifics
Network	☐ Network – Default configurations in use
	☐ Network – Default passwords in use
	☐ Network – Default/common ports allowed or in use
	☐ Network – Network accounts have weak passwords
	☒ Network – No ACLs present/in-use
	☐ Network – No anti-virus/anti-malware
	☐ Network – No encryption
	☐ Network – No firewall present
	☒ Network – No ingress/egress filtering
	☒ Network – No network segmentation
	☐ Network – No secured remote access
	☒ Network – No security monitoring
	☐ Network – No separate POS environment
	☐ Network – No/insufficient logging
	☐ Network – Use of insecure protocols

Vector Type	Specifics
Remote Access	☒ Remote Access – No monitoring/logging of remote access
	☐ Remote Access – Out-dated/known vulnerable hardware/software in use
	☐ Remote Access – Remote access forwarding allowed
	☒ Remote Access – Remote access left permanently enabled
	☐ Remote Access – Unrestricted remote access allowed
	☐ Remote Access – Use of blackbox/proprietary hardware/software

Vector Type	Specifics
Remote Access	☐ Remote Access – Use of default passwords/accounts
	☐ Remote Access – Use of default/out-of-box configuration
	☐ Remote Access – Use of insecure remote software (e.g., VNC)
	☐ Remote Access – Use of known POS vendor defaults
	☐ Remote Access – Use of weak passwords
	☐

Vector Type	Specifics
Web Attack	☐ Web Attack – Allocation of Resources Without Limits or Throttling
	☐ Web Attack – Buffer Access with Incorrect Length Value
	☐ Web Attack – Buffer Copy without Checking Size of Input (Classic Buffer Overflow)
	☐ Web Attack – Cross-site Request Forgery (CSRF)
	☐ Web Attack – Download of Code Without Integrity Check
	☐ Web Attack – Improper Access Control (Authorization)
	☐ Web Attack – Improper Check for Unusual or Exceptional Conditions
	☐ Web Attack – Improper Control of Filename for Include/Require Statement in PHP Program (PHP File Inclusion)
	☐ Web Attack – Unrestricted Upload of File with Dangerous Type
	☐ Web Attack – Improper Sanitization of Special Elements used in an OS Command (OS Command Injection)
	☐ Web Attack – Use of a Broken or Risky Cryptographic Algorithm
	☐ Web Attack – Improper Validation of Array Index
	☐ Web Attack – Incorrect Calculation of Buffer Size

Vector Type	Specifics
Web Attack	☐ Web Attack – Incorrect Permission Assignment for Critical Resource
	☐ Web Attack – Information Exposure Through an Error Message
	☐ Web Attack – Integer Overflow or Wraparound
	☐ Web Attack – Missing Authentication for Critical Function
	☐ Web Attack – Missing Encryption of Sensitive Data
	☐ Web Attack – Race Condition
	☐ Web Attack – Reliance on Untrusted Inputs in a Security Decision
	☐ Web Attack – Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
	☐ Web Attack – URL Redirection to Untrusted Site (Open Redirect)
	☐ Web Attack – Improper Sanitization of Special Elements used in an SQL Command (SQL Injection)
	☐ Web Attack – Use of Hard-coded Credentials
	☐ Web Attack – Failure to Preserve Web Page Structure (Crosssite Scripting)

Appendix E: Supporting Evidence

E.1 Prefetch – v5.exe & artifact.exe

SYSTEM	SUMMARY
GlobalKitchen : GK_POS_SERVER	Prefetch files are used by the operating system to speed up the loading time for application. When application are executed for the first time *Microsoft Windows* creates prefetch files for the application. The following prefetch file illustrates POS malware executing on the system utilizing the v5.exe and artifact.exe binary.

Host	Prefetch File	C-Time	M-Time	Executable Path
GlobalKitchen : GK_POS_SERVER	05988060.pf	11/05/14 11:03 AM	12/17/16 01:08 PM	C:\INNOASXP\System32\1025\1\v5.exe
GlobalKitchen : GK_POS_SERVER	05974983.pf	11/05/14 11:03 AM	12/17/16 01:07 PM	C:\INNOASXP\System32\1025\1\artifact.exe

E.2 Local Password Settings

SYSTEM	SUMMARY
ALL Reviewed	The following information was extracted from the *SAM* registry hive. The entries indicate that not all the local admin passwords are changed on a regular basis. Furthermore, a password is not required for either the *Administrator* or *USER* users. Only the settings from a single system are listed below. However, all systems reviewed had similar settings.

```
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Mon May  7 23:50:30 2012 Z
Last Login Date : Fri Sep 16 02:33:07 2011 Z
Pwd Reset Date  : Fri Sep 16 02:22:44 2011 Z
Pwd Fail Date   : Thu Apr 20 08:04:27 2017 Z
Login Count     : 7
  --> Account Disabled
  --> Password not required
  --> Password does not expire
  --> Normal user account
```

```
Username        : USER [1001]
Full Name       : INNOAS
User Comment    :
Account Type    : Default Admin User
Account Created : Fri Feb 17 00:14:46 2017 Z
Password Hint   :
Last Login Date : Wed Jun  7 00:29:46 2017 Z
Pwd Reset Date  : Mon Feb 13 16:21:29 2017 Z
Pwd Fail Date   : Thu Apr 20 08:08:26 2017 Z
Login Count     : 2513
  --> Password not required
  --> Password does not expire
  --> Normal user account
```

E.3 Audit Subsystem

SYSTEM	SUMMARY
ALL Reviewed	The *SECURITY* hive simply records which events are being audited, or logged in the *Microsoft Windows* event logs. The registry settings below indicate that auditing is disabled. These settings were found on all systems reviewed.

```
auditpol
Policy\PolAdtEv
LastWrite Time Fri Dec 10 18:06:21 2010 (UTC)

Length of data: 138 bytes.
0x00000000: 00 01 00 00 09 00 30 77 78 00 00 00 01 00 00 00  ......0wx.......
0x00000010: 03 00 00 00 03 00 01 00 01 00 01 00 00 00 01 00  ................
0x00000020: 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00  ................
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00  ................
0x00000050: 01 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00  ................
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00000070: 00 00 00 00 00 00 00 00 05 00 09 00 0c 00 03 00  ................
0x00000080: 04 00 06 00 06 00 04 00 04 00                    ..........
**Auditing is NOT enabled.
```

E.4 Windows Version

SYSTEM	SUMMARY
GlobalKitchen : GK_POS7	The *SOFTWARE* hive contains data regarding software installed on the system. The keys below indicate that the operating system installed on this system are out of date.

```
(Software) Get Windows version

ProductName = Microsoft Windows XP
CSDVersion  = Service Pack 3
InstallDate = Tue Jan 17 22:10:10 2017
```

E.5 License Key Generators/Crack Programs

SYSTEM	SUMMARY
ALL Reviewed	While it is unclear if this program has been executed, Foregenix discovered within a setup folder what *Virustotal* classified as malicious key generation / crack programs. Applications of this nature put merchant's at risks due to the uncertainty of their validity. Below are examples of which were present.

```
File: POS-8\D\INNOAS SETUP\ER Tools\R-Studio\crack.exe
File: POS-7\C\INNOAS SYS\Portable Programs\R-Studio\crack.exe
File: POS\D\INNOAS SETUP\ER Tools\R-Studio\crack.exe
File: SERVER\D\INNOAS SETUP\ER Tools\R-Studio\crack.exe
Hash: 91282af5d20982be7b617979ac2833e4

File: ERVER\D\INNOAS SETUP\REQ\AIDA64\chili-KEYGEN.exe
File: POS-2\D\INNOAS SETUP\REQ\AIDA64\chili-KEYGEN.exe
File: POS-6\D\INNOAS SETUP\REQ\AIDA64\chili-KEYGEN.exe
File: POS-1\D\INNOAS SETUP\REQ\AIDA64\chili-KEYGEN.exe
Hash: 8d61f18d4de89d6f14121ccaf113db1a
```

E.6 Screen Capture of Unauthorized use of *LogMeIn*

SYSTEM	SUMMARY
INNOAS-SERVER	The following image is a screenshot from a video which Foregenix obtained from INNOAS, Inc.. The video was a recording of an unauthorized user logging in from 64.120.44.139 [Phoenix Arizona].

E.7 LogMeIn Access Logs

SUMMARY							
Location	User	Start Date	Start Time	Stop Date	Stop Time	Total Time	Source IP
BBQ - Cliffside Park - KEO BOO KEE, Corp	acc@innoas.com	2016-12-13	3:34:02	2016-12-13	3:40:59	0h:6m:57s	64.120.44.139
BBQ - Cliffside Park - KEO BOO KEE, Corp	acc@innoas.com	2016-12-13	3:34:03	2016-12-13	3:57:27	0h:23m:24s	64.120.44.139
BBQ - Cliffside Park - KEO BOO KEE, Corp	acc@innoas.com	2016-12-15	5:05:34	2016-12-15	5:25:33	0h:19m:59s	64.120.44.139
BBQ - Cliffside Park - KEO BOO KEE, Corp	acc@innoas.com	2016-12-17	9:16:07	2016-12-17	9:18:09	0h:2m:2s	64.120.44.139
BBQ - Flushing - Lee & Lim, LLC	acc@innoas.com	2016-12-09	15:01:21	2016-12-09	15:12:14	0h:10m:53s	64.120.44.139
BBQ - Flushing - Lee & Lim, LLC	acc@innoas.com	2016-12-15	5:05:33	2016-12-15	5:23:45	0h:18m:12s	64.120.44.139
BBQ - Flushing - Lee & Lim, LLC	acc@innoas.com	2016-12-17	9:13:01	2016-12-17	9:20:10	0h:7m:9s	64.120.44.139
BBQ - Old Tappan - Kenny Baek, Corp	acc@innoas.com	2016-12-15	5:23:47	2016-12-15	5:39:50	0h:16m:3s	64.120.44.139
Bocca Bliss - 725 Third Avenue Corp	acc@innoas.com	2016-12-17	7:56:45	2016-12-17	8:07:00	0h:10m:15s	64.120.44.139
Bocca Bliss - 726 Third Avenue Corp	acc@innoas.com	2016-12-17	7:56:48	2016-12-17	7:57:33	0h:0m:45s	64.120.44.139
Bocca Bliss - 727 Third Avenue Corp	acc@innoas.com	2016-12-17	7:56:49	2016-12-17	8:15:11	0h:18m:22s	64.120.44.139
Boom Boom Edison - BC of God	acc@innoas.com	2016-12-17	9:49:35	2016-12-17	10:03:25	0h:13m:50s	64.120.44.139
Caffe Bene 157th St - House of Caffe Bene, Inc	acc@innoas.com	2016-12-14	4:06:52	2016-12-14	4:25:38	0h:18m:46s	64.120.44.139
Caffe Bene 157th St - House of Caffe Bene, Inc	acc@innoas.com	2016-12-15	5:38:15	2016-12-15	5:46:23	0h:8m:8s	64.120.44.139
Caffe Bene 32nd ST (No POS use)	acc@innoas.com	2016-12-15	5:38:17	2016-12-15	5:54:40	0h:16m:23s	64.120.44.139
Caffe Bene Astoria (Business Closed)	acc@innoas.com	2016-12-15	5:38:18	2016-12-15	5:49:46	0h:11m:28s	64.120.44.139
Caffe Bene Boston - Chen & Chen Brothers, Inc	acc@innoas.com	2016-12-10	8:11:01	2016-12-10	8:29:15	0h:18m:14s	64.120.44.139
Caffe Bene Boston - Chen & Chen Brothers, Inc	acc@innoas.com	2016-12-13	4:01:14	2016-12-13	4:05:51	0h:4m:37s	64.120.44.139
Caffe Bene Boston - Chen & Chen Brothers, Inc	acc@innoas.com	2016-12-14	1:47:02	2016-12-14	1:54:59	0h:7m:57s	64.120.44.139
Caffe Bene Boston - Chen & Chen Brothers, Inc	acc@innoas.com	2016-12-14	1:47:05	2016-12-14	2:01:14	0h:14m:9s	64.120.44.139
Caffe Bene Boston - Chen & Chen Brothers, Inc	acc@innoas.com	2016-12-14	1:52:56	2016-12-14	2:00:35	0h:7m:39s	64.120.44.139

Location	User	Start Date	Start Time	Stop Date	Stop Time	Total Time	Source IP
Caffe Bene Boston - Chen & Chen Brothers, Inc	acc@innoas.com	2016-12-15	3:56:50	2016-12-15	3:58:52	0h:2m:2s	64.120.44.139
Caffe Bene Brooklyn 18th - Lucky Star Caffe, Inc	acc@innoas.com	2016-12-17	6:37:16	2016-12-17	7:10:56	0h:33m:40s	64.120.44.139
Caffe Bene Brooklyn 19th - Lucky Star Caffe, Inc	acc@innoas.com	2016-12-10	9:16:45	2016-12-10	9:18:42	0h:1m:57s	64.120.44.139
Caffe Bene Buena Park - Bae&Kim, Inc	acc@innoas.com	2016-12-13	4:21:44	2016-12-13	4:37:13	0h:15m:29s	64.120.44.139
Caffe Bene Buena Park - Bae&Kim, Inc	acc@innoas.com	2016-12-14	5:28:31	2016-12-14	5:33:07	0h:4m:36s	64.120.44.139
Caffe Bene Buena Park - Bae&Kim, Inc	acc@innoas.com	2016-12-16	3:16:41	2016-12-16	3:25:56	0h:9m:15s	64.120.44.139
Caffe Bene Buena Park - Bae&Kim, Inc	acc@innoas.com	2016-12-16	4:38:46	2016-12-16	4:42:40	0h:3m:54s	64.120.44.139
Caffe Bene Buena Park - Bae&Kim, Inc	acc@innoas.com	2016-12-16	4:45:14	2016-12-16	4:55:07	0h:9m:53s	64.120.44.139
Caffe Bene Buena Park - Bae&Kim, Inc	acc@innoas.com	2016-12-17	5:48:46	2016-12-17	5:56:24	0h:7m:38s	64.120.44.139
Caffe Bene Carrollton - Carrot House Inc	acc@innoas.com	2016-12-10	7:55:27	2016-12-10	8:09:12	0h:13m:45s	64.120.44.139
Caffe Bene Carrollton - Carrot House Inc	acc@innoas.com	2016-12-14	1:59:34	2016-12-14	2:14:24	0h:14m:50s	64.120.44.139
Caffe Bene Carrollton - Carrot House Inc	acc@innoas.com	2016-12-16	3:27:57	2016-12-16	3:37:06	0h:9m:9s	64.120.44.139
Caffe Bene Chamapaign - Caffe Bene Green Inc	acc@innoas.com	2016-12-10	9:16:50	2016-12-10	9:17:49	0h:0m:59s	64.120.44.139
Caffe Bene Chamapaign - Caffe Bene Green Inc	acc@innoas.com	2016-12-10	9:24:34	2016-12-10	9:37:33	0h:12m:59s	64.120.44.139
Caffe Bene Chamapaign - Caffe Bene Green Inc	acc@innoas.com	2016-12-13	4:35:45	2016-12-13	4:51:20	0h:15m:35s	64.120.44.139
Caffe Bene Chamapaign - Caffe Bene Green Inc	acc@innoas.com	2016-12-17	6:58:27	2016-12-17	7:15:24	0h:16m:57s	64.120.44.139
Caffe Bene Chamapaign - Caffe Bene Green Inc	acc@innoas.com	2016-12-17	9:20:08	2016-12-17	9:22:06	0h:1m:58s	64.120.44.139
Caffe Bene Ellicott City - Abies Corp	acc@innoas.com	2016-12-10	8:11:16	2016-12-10	8:23:01	0h:11m:45s	64.120.44.139
Caffe Bene Ellicott City - Abies Corp	acc@innoas.com	2016-12-13	4:21:40	2016-12-13	4:24:28	0h:2m:48s	64.120.44.139
Caffe Bene Ellicott City - Abies Corp	acc@innoas.com	2016-12-15	3:56:59	2016-12-15	4:06:42	0h:9m:43s	64.120.44.139
Caffe Bene Ellicott City - Abies Corp	acc@innoas.com	2016-12-15	6:16:13	2016-12-15	6:21:55	0h:5m:42s	64.120.44.139
Caffe Bene Ellicott City - Abies Corp	acc@innoas.com	2016-12-16	4:36:18	2016-12-16	4:41:16	0h:4m:58s	64.120.44.139
Caffe Bene Ellicott City - Abies Corp	acc@innoas.com	2016-12-17	5:54:50	2016-12-17	6:01:17	0h:6m:27s	64.120.44.139
Caffe Bene Fort Lee - Caffe Bene Fort Lee, Inc	acc@innoas.com	2016-12-14	3:15:20	2016-12-14	3:49:47	0h:34m:27s	64.120.44.139

Location	User	Start Date	Start Time	Stop Date	Stop Time	Total Time	Source IP
Caffe Bene Fort Lee - Caffe Bene Fort Lee, Inc	acc@innoas.com	2016-12-15	6:20:33	2016-12-15	6:29:13	0h:8m:40s	64.120.44.139
Caffe Bene Glenview - Caffe Bene Midwest LLC	acc@innoas.com	2016-12-13	4:01:05	2016-12-13	4:11:33	0h:10m:28s	64.120.44.139
Caffe Bene Glenview - Caffe Bene Midwest LLC	acc@innoas.com	2016-12-14	3:15:26	2016-12-14	3:36:49	0h:21m:23s	64.120.44.139
Caffe Bene Glenview - Caffe Bene Midwest LLC	acc@innoas.com	2016-12-14	4:06:46	2016-12-14	4:12:21	0h:5m:35s	64.120.44.139
Caffe Bene Jersey City - Pak Café Bene, LLC	acc@innoas.com	2016-12-15	5:38:15	2016-12-15	5:49:10	0h:10m:55s	64.120.44.139
Caffe Bene Jersey City - Pak Café Bene, LLC	acc@innoas.com	2016-12-17	6:15:59	2016-12-17	6:31:56	0h:15m:57s	64.120.44.139
Caffe Bene MPD - CB 17th Street, LLC	acc@innoas.com	2016-12-17	6:37:31	2016-12-17	6:48:35	0h:11m:4s	64.120.44.139
Caffe Bene MPD - CB 18th Street, LLC	acc@innoas.com	2016-12-15	4:35:08	2016-12-15	4:46:41	0h:11m:33s	64.120.44.139
Caffe Bene MPD - CB 19th Street, LLC	acc@innoas.com	2016-12-13	4:55:40	2016-12-13	5:00:17	0h:4m:37s	64.120.44.139
Caffe Bene MPD - CB 20th Street, LLC	acc@innoas.com	2016-12-10	8:30:32	2016-12-10	9:04:47	0h:34m:15s	64.120.44.139
Caffe Bene New Brunswick - Soonmyung Development Corp	acc@innoas.com	2016-12-14	4:06:52	2016-12-14	4:23:55	0h:17m:3s	64.120.44.139
Caffe Bene Rowland Hts - JihoJiwwo, Inc	acc@innoas.com	2016-12-10	8:30:14	2016-12-10	8:43:19	0h:13m:5s	64.120.44.139
Caffe Bene Rowland Hts - JihoJiwwo, Inc	acc@innoas.com	2016-12-13	4:55:48	2016-12-13	4:59:39	0h:3m:51s	64.120.44.139
Caffe Bene Rowland Hts - JihoJiwwo, Inc	acc@innoas.com	2016-12-14	5:28:37	2016-12-14	5:37:17	0h:8m:40s	64.120.44.139
Caffe Bene Rowland Hts - JihoJiwwo, Inc	acc@innoas.com	2016-12-16	3:16:49	2016-12-16	3:29:19	0h:12m:30s	64.120.44.139
Caffe Bene Rowland Hts - JihoJiwwo, Inc	acc@innoas.com	2016-12-17	5:59:35	2016-12-17	6:13:20	0h:13m:45s	64.120.44.139
Caffe Bene Rowland Hts - JihoJiwwo, Inc	acc@innoas.com	2016-12-17	6:11:56	2016-12-17	6:12:02	0h:0m:6s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-09	13:59:37	2016-12-09	14:04:07	0h:4m:30s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-09	14:02:49	2016-12-09	14:29:07	0h:26m:18s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-10	9:16:42	2016-12-10	9:18:58	0h:2m:16s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-10	9:24:30	2016-12-10	9:44:14	0h:19m:44s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-15	4:35:08	2016-12-15	4:47:20	0h:12m:12s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-16	3:17:01	2016-12-16	3:29:38	0h:12m:37s	64.120.44.139
Caffe Bene San Diego - MCKN Enterprise, Inc	acc@innoas.com	2016-12-17	6:37:14	2016-12-17	6:53:49	0h:16m:35s	64.120.44.139

Location	User	Start Date	Start Time	Stop Date	Stop Time	Total Time	Source IP
Caffe Bene San Marino - San Marino Caffebene, Inc	acc@innoas.com	2016-12-09	15:52:58	2016-12-09	15:58:30	0h:5m:32s	64.120.44.139
Caffe Bene San Marino - San Marino Caffebene, Inc	acc@innoas.com	2016-12-10	9:16:48	2016-12-10	9:40:07	0h:23m:19s	64.120.44.139
Caffe Bene San Marino - San Marino Caffebene, Inc	acc@innoas.com	2016-12-13	4:21:54	2016-12-13	4:27:29	0h:5m:35s	64.120.44.139
Caffe Bene San Marino - San Marino Caffebene, Inc	acc@innoas.com	2016-12-16	3:16:57	2016-12-16	3:25:55	0h:8m:58s	64.120.44.139
Caffe Bene San Marino - San Marino Caffebene, Inc	acc@innoas.com	2016-12-17	6:58:27	2016-12-17	7:08:48	0h:10m:21s	64.120.44.139
Caffe Bene San Marino - San Marino Caffebene, Inc	acc@innoas.com	2016-12-17	9:20:10	2016-12-17	9:22:15	0h:2m:5s	64.120.44.139
Caffe Bene Sunnyside - June & Shana, Inc	acc@innoas.com	2016-12-14	3:15:28	2016-12-14	4:02:58	0h:47m:30s	64.120.44.139
Caffe Bene Sunnyside - June & Shana, Inc	acc@innoas.com	2016-12-14	4:06:43	2016-12-14	4:12:51	0h:6m:8s	64.120.44.139
Caffe Bene Suwanee - Kim Crystal Min, Inc	acc@innoas.com	2016-12-10	8:30:25	2016-12-10	9:14:54	0h:44m:29s	64.120.44.139
Caffe Bene Suwanee - Kim Crystal Min, Inc	acc@innoas.com	2016-12-13	4:35:36	2016-12-13	4:39:41	0h:4m:5s	64.120.44.139
Caffe Bene Suwanee - Kim Crystal Min, Inc	acc@innoas.com	2016-12-14	5:28:43	2016-12-14	5:38:58	0h:10m:15s	64.120.44.139
Caffe Bene Suwanee - Kim Crystal Min, Inc	acc@innoas.com	2016-12-15	4:35:11	2016-12-15	4:44:58	0h:9m:47s	64.120.44.139
Caffe Bene Suwanee - Kim Crystal Min, Inc	acc@innoas.com	2016-12-17	6:16:03	2016-12-17	6:35:36	0h:19m:33s	64.120.44.139
Caffe Bene Urbana - Caffe Bene Champaign, Inc	acc@innoas.com	2016-12-13	4:01:03	2016-12-13	4:13:19	0h:12m:16s	64.120.44.139
Caffe Bene Western - Nabee Inc	acc@innoas.com	2016-12-10	8:07:32	2016-12-10	8:18:12	0h:10m:40s	64.120.44.139
Caffe Bene Western - Nabee Inc	acc@innoas.com	2016-12-14	2:25:35	2016-12-14	2:33:39	0h:8m:4s	64.120.44.139
Caffe Bene Western - Nabee Inc	acc@innoas.com	2016-12-14	2:39:06	2016-12-14	2:43:53	0h:4m:47s	64.120.44.139
Caffe Bene Western - Nabee Inc	acc@innoas.com	2016-12-16	3:27:56	2016-12-16	3:45:44	0h:17m:48s	64.120.44.139
Caffe Bene Wilshire - Kafferia, Inc	acc@innoas.com	2016-12-14	1:59:39	2016-12-14	2:23:54	0h:24m:15s	64.120.44.139
Caffe Bene Wilshire - Kafferia, Inc	acc@innoas.com	2016-12-14	2:25:38	2016-12-14	2:40:42	0h:15m:4s	64.120.44.139
Caffe Bene Wilshire - Kafferia, Inc	acc@innoas.com	2016-12-16	3:28:00	2016-12-16	3:46:26	0h:18m:26s	64.120.44.139
Casino Car Wash	acc@innoas.com	2016-12-09	13:40:31	2016-12-09	13:50:46	0h:10m:15s	64.120.44.139
Cast Iron Pot - Pinnacle Bar&Grill	acc@innoas.com	2016-12-17	7:26:56	2016-12-17	7:39:11	0h:12m:15s	64.120.44.139
Cast Iron Pot - Pinnacle Bar&Grill	acc@innoas.com	2016-12-17	7:26:58	2016-12-17	7:41:51	0h:14m:53s	64.120.44.139

Location	User	Start Date	Start Time	Stop Date	Stop Time	Total Time	Source IP
Cast Iron Pot - Pinnacle Bar&Grill	acc@innoas.com	2016-12-17	7:26:59	2016-12-17	7:45:40	0h:18m:41s	64.120.44.139
Cast Iron Pot - Pinnacle Bar&Grill	acc@innoas.com	2016-12-17	7:27:01	2016-12-17	7:50:03	0h:23m:2s	64.120.44.139
Cast Iron Pot - Pinnacle Bar&Grill	acc@innoas.com	2016-12-17	7:27:03	2016-12-17	7:55:02	0h:27m:59s	64.120.44.139
Classique Day Spa (No POS Use)	acc@innoas.com	2016-12-15	4:53:47	2016-12-15	5:04:26	0h:10m:39s	64.120.44.139
Crome Fort Lee - Namgung Corp	acc@innoas.com	2016-12-10	4:50:33	2016-12-10	5:12:35	0h:22m:2s	64.120.44.139
Crome Fort Lee - Namgung Corp	acc@innoas.com	2016-12-10	5:15:50	2016-12-10	6:15:57	1h:0m:7s	64.120.44.139
Crome Fort Lee - Namgung Corp	acc@innoas.com	2016-12-17	9:32:01	2016-12-17	9:48:48	0h:16m:47s	64.120.44.139
Crome Fort Lee - Namgung Corp	acc@innoas.com	2016-12-17	9:49:33	2016-12-17	9:59:09	0h:9m:36s	64.120.44.139
Global Kitchen (GKNY1 Inc)	acc@innoas.com	2016-12-16	4:18:14	2016-12-16	4:34:29	0h:16m:15s	64.120.44.139
Global Kitchen (GKNY2 Inc)	acc@innoas.com	2016-12-16	3:50:15	2016-12-16	4:13:21	0h:23m:6s	64.120.44.139
Global Kitchen (GKNY3 Inc)	acc@innoas.com	2016-12-17	7:57:35	2016-12-17	8:11:21	0h:13m:46s	64.120.44.139
Global Kitchen (GKNY4 Inc)	acc@innoas.com	2016-12-16	3:50:11	2016-12-16	4:00:24	0h:10m:13s	64.120.44.139
Global Kitchen (GKNY5 Inc)	acc@innoas.com	2016-12-17	8:32:03	2016-12-17	8:43:54	0h:11m:51s	64.120.44.139
Global Kitchen (GKNY6 Inc)	acc@innoas.com	2016-12-16	4:17:09	2016-12-16	4:34:53	0h:17m:44s	64.120.44.139
Global Kitchen (GKNY7 Inc)	acc@innoas.com	2016-12-16	3:50:22	2016-12-16	4:12:41	0h:22m:19s	64.120.44.139
Izakaya Nomad - Jamo 26, Inc	acc@innoas.com	2016-12-17	9:30:58	2016-12-17	9:38:02	0h:7m:4s	64.120.44.139
Izakaya Nomad - Jamo 27, Inc	acc@innoas.com	2016-12-10	6:26:50	2016-12-10	6:52:19	0h:25m:29s	64.120.44.139
Piccola Cucina - Spring R & G Soho, LLC	acc@innoas.com	2016-12-10	6:29:27	2016-12-10	7:13:40	0h:44m:13s	64.120.44.139
Piccola Cucina - Spring R & G Soho, LLC	acc@innoas.com	2016-12-13	5:22:04	2016-12-13	5:27:27	0h:5m:23s	64.120.44.139
Piccola Cucina - Spring R & G Soho, LLC	acc@innoas.com	2016-12-15	3:29:50	2016-12-15	3:40:22	0h:10m:32s	64.120.44.139
Piccola Cucina - Spring R & G Soho, LLC	acc@innoas.com	2016-12-17	9:00:04	2016-12-17	9:08:22	0h:8m:18s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-10	6:29:23	2016-12-10	6:53:13	0h:23m:50s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-10	6:29:30	2016-12-10	6:50:33	0h:21m:3s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-13	5:17:19	2016-12-13	5:24:51	0h:7m:32s	64.120.44.139

Location	User	Start Date	Start Time	Stop Date	Stop Time	Total Time	Source IP
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-13	5:22:02	2016-12-13	5:32:30	0h:10m:28s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-15	3:29:47	2016-12-15	3:42:57	0h:13m:10s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-15	3:29:52	2016-12-15	3:41:24	0h:11m:32s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-17	9:00:01	2016-12-17	9:11:29	0h:11m:28s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-17	9:00:09	2016-12-17	9:13:09	0h:13m:0s	64.120.44.139
Piccola Cucina Miami - R & G Espanola, LLC	acc@innoas.com	2016-12-17	9:11:38	2016-12-17	9:16:47	0h:5m:9s	64.120.44.139
Piccola Cucina Prince - R & G Soho, LLC	acc@innoas.com	2016-12-17	8:32:08	2016-12-17	8:47:11	0h:15m:3s	64.120.44.139
Piccola Cucina Prince - R & G Soho, LLC	acc@innoas.com	2016-12-17	11:20:26	2016-12-17	11:25:15	0h:4m:49s	64.120.44.139
Rokman - PHK Co, Inc	acc@innoas.com	2016-12-09	15:39:18	2016-12-09	15:42:14	0h:2m:56s	64.120.44.139
Rokman - PHK Co, Inc	acc@innoas.com	2016-12-10	7:42:23	2016-12-10	7:47:02	0h:4m:39s	64.120.44.139
Rokman - PHK Co, Inc	acc@innoas.com	2016-12-10	7:42:25	2016-12-10	7:52:03	0h:9m:38s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-10	6:51:31	2016-12-10	7:09:22	0h:17m:51s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-10	6:51:42	2016-12-10	7:21:43	0h:30m:1s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-10	6:51:45	2016-12-10	7:18:09	0h:26m:24s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-13	5:21:58	2016-12-13	5:28:43	0h:6m:45s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-17	9:18:45	2016-12-17	9:30:28	0h:11m:43s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-17	9:18:49	2016-12-17	9:32:39	0h:13m:50s	64.120.44.139
Soju Haus (No Pos Use)	acc@innoas.com	2016-12-17	9:18:50	2016-12-17	9:27:12	0h:8m:22s	64.120.44.139
Wally's - Wally's Hot Bagles, LLC	acc@innoas.com	2016-12-17	8:13:54	2016-12-17	8:20:33	0h:6m:39s	64.120.44.139
Wally's - Wally's Hot Bagles, LLC	acc@innoas.com	2016-12-17	8:13:55	2016-12-17	8:21:18	0h:7m:23s	64.120.44.139
Wally's - Wally's Hot Bagles, LLC	acc@innoas.com	2016-12-17	8:25:36	2016-12-17	8:31:37	0h:6m:1s	64.120.44.139

Document Control

Document Control	Draft Version	0.1	2017-07-26	Sterling Thomas
	Draft Version	0.2	2017-08-01	Sterling Thomas
	QA Review	0.5	2017-08-10	Foregenix QA
	FINAL Release	1.0	2017-09-05	Chris Hague
Distribution	American Express Contact		Steve Marquis	
	Mastercard Contact		Christopher Bennett Anastasia Nitis	
	VISA Inc. Contact		Stoddard Lambertson	
	Discover Contact		Stacey Baisden	
	JCB Contact		Lib DeVeyra	
	Primary Project Contact		Jake Lee	
	Acquirer Contact		Not applicable	
	Foregenix DFIR Director		Andrew Bontoft	
	Foregenix Account Manager		Benjamin Hosack	